IVANTI NEURONS FOR UEM | AUDIT TRAILS

Securing your Azure Blob Storage

How Shared Access Signature (SAS) tokens protect the audit logs you export to your SIEM

A reference for administrators using the Azure Blob Storage SIEM Forwarding Connector with Ivanti Neurons.

How your audit logs are secured

Ivanti Neurons can forward your audit trail logs to a Microsoft Azure Blob Storage container that you own, using the Azure Blob Storage SIEM Forwarding Connector. From there, your SIEM ingests the data through its existing pipeline. A common question is how to keep that storage secure, and in particular how to avoid opening it to the public internet. The connector already protects your container using an Azure Shared Access Signature (SAS) token. This is the same mechanism Microsoft recommends for granting storage access securely.

Access to your container is granted by a signed, write-scoped token, not by the IP address of the sender. This is why you do not need to allow the public internet to read your storage, and why locking the account to a fixed list of IP addresses is not the right tool.

What is a SAS token?

A Shared Access Signature is a special web link (a URL) that grants limited, temporary access to your storage. It is signed using your storage account key, so it cannot be forged. It does not expose the account key itself, it works only over a secure HTTPS connection, and it stops working automatically when it expires. In short, it is a key that opens one door, for one task, for a limited time. For the SIEM connector, that door is write access to your chosen container, so Neurons can deliver logs and nothing more.

Where this is documented

Both of these answers are set out in the official Ivanti documentation:

- Azure Blob Storage SIEM Forwarding Connector
- Audit Trails overview (access methods and comparison)

How the connector uses SAS

The connector runs in the cloud and writes to your storage on a schedule. You set it up once, under Admin > Connectors in the Neurons console.

1. In the Azure portal, create or select a storage account and a blob container to receive the logs. Use **Account key** as the signing method for the container.

2. Generate a **Blob SAS URL** for that container with **write** permission, set to **HTTPS only**, with an expiry date set well into the future so delivery is not interrupted.

3. In the Neurons console, add the Azure Blob Storage SIEM Forwarding Connector, paste the Blob SAS URL, set how often logs are exported (every 30, 45 or 60 minutes), then use **Test Connections** and **Save**. The connector saves only after the test succeeds.

4. Neurons periodically writes your audit logs to the container in JSON format. Your SIEM then ingests them from your own storage using its normal method.

Only the Neurons platform connects to your storage, and only to write. Your managed devices are never involved in this flow. Because the SAS signature authorises each write, the IP address the platform connects from is not the security boundary.

The two most common questions

These are the two questions administrators raise most often when hardening their storage for audit-log forwarding.

1. Which IP addresses will Neurons connect from, so we can apply least privilege?

Least privilege on your storage account is achieved through the SAS token, not through an IP allowlist. The connector authenticates with a Blob SAS URL that you scope to a single container, limit to write permission, and restrict to HTTPS. That is the narrowest access the platform needs, and it cannot be forged or reused elsewhere.

The export runs from the Neurons platform in the cloud, and its outbound addresses are dynamic and open-ended rather than a fixed, published range. For that reason, restricting the storage account firewall to a fixed list of IP addresses is not workable and is not supported. If your policy strictly requires a fixed source-IP allowlist, that would need a product enhancement request, which your Ivanti contact can raise on your behalf.

2. Can we pull the logs from an API instead of Ivanti pushing them?

Ivanti Neurons uses a push model for audit logs. The platform writes the logs to a destination that you own and control, and your systems read them from there. There is no Ivanti-hosted endpoint that your ingestion application polls directly.

In practice this gives you the pull behaviour you are after. Your ingestion application reads from your own Azure Blob Storage container, on your own schedule. The container is the handover point: Neurons writes, your application or SIEM reads.

If Azure Blob Storage is not your preferred destination, the same audit data can be forwarded to Splunk through the Splunk HEC connector or to an Amazon S3 bucket, or exported as a scheduled CSV report covering up to 90 days and delivered by email. See the Audit Trails overview for the full comparison.

Network access is not the same as anonymous access

The word public is used for two different Azure settings, and they are easy to confuse. Understanding the difference is the key to securing your storage correctly.

Azure setting	What it controls	What the connector needs
Public network access (Networking)	Whether the storage endpoint can be reached over the internet at all.	Must be enabled. The Neurons platform reaches your container over the public endpoint to write the logs.
Anonymous blob access (Configuration)	Whether anyone can read your files without any credentials.	Not required. The SAS token authorises every write, so your container can stay private.

Why a fixed IP list is not the right control

Only the Neurons platform writes to your container, and it does so from cloud egress addresses that are dynamic and open-ended. Ivanti does not publish a fixed source-IP list for the outbound connector, so a storage-account firewall pinned to a fixed set of addresses would block delivery. The write-scoped SAS token is the control that keeps the container private while still letting Neurons deliver your logs.

Recommended hardening

- Use a storage account dedicated to audit-log forwarding, so nothing else shares its exposure.
- Enable Secure transfer required on the storage account, so only HTTPS connections are accepted.
- Keep your container private. The SAS token provides the access Neurons needs.
- Scope the SAS to a single container and to write permission only. This is the least privilege the connector requires.
- Restrict the SAS to the HTTPS protocol, and set a realistic expiry. Note that forwarding stops when the SAS expires, so plan to renew it before that date.
- Remember that rotating the storage account key invalidates any SAS signed with that key. Regenerate and re-enter the SAS URL after a key rotation.

Not supported

A Private Endpoint on the storage account is not supported, because it prevents the Neurons platform from reaching your container to write the logs. Restricting the account firewall to a fixed set of IP addresses is also not supported, for the reasons above.

Other ways to access your audit logs

SIEM forwarding is one of several ways to reach your audit data. The right choice depends on how long you need to keep the logs and how you want to consume them.

Method	Retention	Integration	Best use case
Audit Trails (in console)	30 days	None	Immediate troubleshooting and active monitoring.
Audit Trails Report	Up to 90 days	Scheduled CSV by email	Compliance audits, periodic archiving, regular review.
Azure Blob Storage connector	Continuous, every 30 / 45 / 60 min	SIEM via your Azure storage	Central storage, SIEM pipeline integration, log aggregation.
Splunk HEC connector	Continuous, every 30 / 45 / 60 min	Splunk Enterprise	Advanced analytics, correlation, threat detection.
Amazon S3 connector	Continuous, every 30 / 45 / 60 min	Amazon S3 bucket	Storage in S3 for downstream tools such as an ELK stack.

The Azure Blob Storage, Splunk HEC and Amazon S3 connectors all use the same push model: Neurons writes to a destination you own, and your systems read from there.

Start here: learning resources

The links below are the official sources for the answers in this reference. They are a good starting point for your infrastructure and security teams.

Ivanti documentation

Azure Blob Storage SIEM Forwarding Connector

Setting up the connector, the Blob SAS URL, and the Account key signing method.

Audit Trails overview

The access methods, retention, and the comparison of in-console, scheduled report and SIEM forwarding.

Connectors

General guidance on configuring and using connectors in the Neurons Platform.

Required URLs, IP addresses and ports

The platform allowlist, in the Requirements section of the Neurons Platform help. The addresses listed there are dynamic.

Microsoft Learn: how SAS works

Create SAS tokens (step by step)

How to generate a SAS for a container in the Azure portal. This is the guide the Ivanti connector documentation points to.

Grant limited access to data with shared access signatures (SAS)

Microsoft's overview of the SAS model, the token types, and how access is authorised.

If anything here needs clarifying for your environment, your Ivanti support contact can help, and can arrange a short call with your infrastructure team.