IVANTI NEURONS FOR UEM | APP DISTRIBUTION

Securing your Azure Blob Storage

How Shared Access Signature (SAS) tokens protect the software you distribute

A reference for administrators using their own Azure Blob Storage with Ivanti Neurons App Distribution.

How your content is secured

Ivanti Neurons App Distribution can deliver software from your own Microsoft Azure Blob Storage. A common question is how to keep that storage secure, and in particular how to avoid leaving it open to the public internet. App Distribution already protects your files using Azure Shared Access Signature (SAS) tokens. This is the same mechanism Microsoft recommends for sharing storage securely.

What is a SAS token?

A Shared Access Signature is a special web link (a URL) that grants limited, temporary access to a single file in your storage account. 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.

Access to your files is granted by a signed, time-limited token, not by the IP address of the device. 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.

How App Distribution uses SAS

1. You add your Azure storage account keys to the Neurons console under Admin > Credentials. Adding both key1 and key2 lets you rotate keys without interruption. The keys stay in Neurons and are never sent to your devices.
2. When you add a file to a Download action, Neurons uses those keys to create a SAS link for that specific file.
3. Each link is set to expire after seven days, and Neurons renews it automatically every five days, so your devices keep access without any manual work.
4. Your managed devices download the file over HTTPS using that signed link. The signature in the link is what authorises the download.

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 App Distribution needs
Public network access (Networking)	Whether the storage endpoint can be reached over the internet at all.	Must be enabled. Both the Neurons platform and your devices reach the storage over the public endpoint.
Anonymous blob access (Configuration)	Whether anyone can read your files without any credentials.	Not required. The SAS tokens authorise every download, so your containers can stay private.

Why a fixed IP list does not work

The dynamic IP addresses shown in the Ivanti allowlist documentation belong to the Neurons platform, which browses your storage and creates the SAS links. In addition, your managed devices download from wherever they are located, such as the office, home or while travelling. Because both sets of addresses change or are open-ended, restricting the storage account to a fixed list of IP addresses is not workable. Moving to a fixed-IP model would require a product enhancement request.

Recommended hardening

- Use a storage account dedicated to App Distribution, so nothing else shares its exposure.
- Enable Secure transfer required on the storage account, so only HTTPS connections are accepted.
- Keep your containers private. The SAS tokens provide access.
- Add a SHA256 hash to the Download action so the agent verifies file integrity after download.
- Rotate your storage keys periodically. With key1 and key2 both registered, rotation does not interrupt distribution.

Not supported

A Private Endpoint on the storage account is not supported, because it prevents both the console and your devices from reaching the files. Restricting the account firewall to a fixed set of IP addresses is also not supported.

A simpler option: Ivanti cloud storage

If you would prefer not to manage your own storage, Neurons includes built-in Ivanti cloud storage. Each tenant has its own Ivanti-managed container, with no credentials, CORS, anonymous access or IP rules for you to manage. The limits are 10 GB in total and 2 GB per file.

Start here: learning resources

The links below are a good starting point for your infrastructure team to learn how SAS works and how Ivanti Neurons uses it.

Microsoft Learn: how SAS works

Grant limited access to data with shared access signatures (SAS)
An overview of the SAS model, the types of token, and how access is authorised.

Delegate access with a shared access signature
How a SAS URI is constructed and what each part of the token means.

Create SAS tokens (step by step)
How to generate a SAS in the Azure portal or Azure Storage Explorer.

Introduction to SAS (video)
A short visual introduction to the concepts, use cases and best practices.

Use SAS instead of anonymous access
Microsoft's guidance to use a SAS rather than enabling public anonymous read.

Ivanti documentation: App Distribution and storage

App Distribution catalog and the Download action
Using your own cloud storage as a source for distributed software.

Cloud file explorer and credentials
Adding your Azure keys in Admin > Credentials, and how SAS URLs are generated.

Required URLs, IP addresses and ports
The platform allowlist, including the dynamic Azure addresses referenced above.

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