AZURE PREREQUISITES

# Required Resources

The following resources are required in an Azure environment for either the Blocklist Integration and/or the Log Forwarding Integration to work.

* API access to your environment
* Microsoft Web
* Microsoft Insights

## Detailed Steps for the Required Resources

### Create Initial API Access

* Go to Microsoft Entra ID
* Click + Add / App registration
* Name - give it a name
* Leave all other settings at default
  + A screenshot of a computer application

    AI-generated content may be incorrect.
* Click Register
* Post-deployment
  + A screenshot of a computer

    AI-generated content may be incorrect.

### Assign Role to API

* Go to Resource groups
* Click on name of resource group
* Click Access control (IAM)
* Click +Add / Add role assignments
* Role
  + In the search field, enter

**network contributor**

* + Click Network Contributor
    - A screenshot of a computer

      AI-generated content may be incorrect.
  + Click Next
* Members
  + Assign access to – leave default of User, group, or service principal
  + Members – click + Select members
  + In the search field, enter the name of the API access created earlier and click on it
    - A screenshot of a computer

      AI-generated content may be incorrect.
  + Click Select
    - A screenshot of a group

      AI-generated content may be incorrect.
  + Click Review + assign

### Generate API Client Secret

* Go to Microsoft Entra ID
* Go to Manage / App registrations
* Click All applications
* In the search field, enter the name of the API access created earlier and click on it
* Go to Manage / Certificates & secrets
* Click on + New client secret
  + Description - enter a description
  + Expires - select a timeframe suitable for your environment
    - A screenshot of a computer

      AI-generated content may be incorrect.
  + Click Add
* Copy the Value entry (aka client secret) using the copy icon (red arrow) \*\*\*
  + \*\*\* Put in your password manager or safe place. **NOTE: Once you navigate away from this page, the client secret will not be able to be retrieved**
  + A screenshot of a computer

    AI-generated content may be incorrect.

### Register MS Insights and MS Web

* Go to Subscriptions
* Click on the subscription name you want
* Go to Settings / Resource providers
* In the filter by name box, enter

**insights**

* Select microsoft.insights
  + A screenshot of a computer

    AI-generated content may be incorrect.
* Click Register
* In the filter by name field, enter

**web**

* Select Microsoft.Web
  + A screenshot of a computer

    AI-generated content may be incorrect.
* Click Register

# Resources for Log Forwarding Integration

The following additional resources are required for the Log Forwarding Integration:

* Event Hub Namespace
* Event Hub
* Log Analytics Workspace
* Application Insights
* Storage Account
* Subnet Flow Log
* DNS Security Policy (currently in preview for Azure commercial)

## Create Event Hub Namespace

* Go to Event Hubs
* Click + Create
* Basics
  + Subscription - select the correct Subscription
  + Resource group - select the correct resource group
  + Namespace name – enter a name for the namespace
  + Location – select the correct location
  + Pricing tier – select Standard
    - A screenshot of a computer

      AI-generated content may be incorrect.
  + All other settings are default
  + Click Review + create
* Summary – pre-deployment
  + A screenshot of a computer

    AI-generated content may be incorrect.
  + Click Create
* Summary – post-deployment
  + A screenshot of a computer

    AI-generated content may be incorrect.

## Create Event Hub

* Go to Event Hubs
* Click Event Hub Namespace created earlier
* Click + Event Hub
* Basics
  + Name – enter a name for the event hub
  + Retention time – (we suggest 120 hours)
  + Leave all other settings at default
  + Click Review + create
* Summary – pre-deployment
  + A screenshot of a computer

    AI-generated content may be incorrect.
  + Click Create
* Post-deployment
  + A screenshot of a computer

    AI-generated content may be incorrect.

## Create Log Analytics Workspace

* Go to Log Analytics workspaces
* Click + Create
* Basics
  + Subscription - select the correct Subscription
  + Resource group - select the correct resource group
  + Name – enter a name for the log analytics workspace
  + Region – select your region (same as location)
    - A screenshot of a computer screen

      AI-generated content may be incorrect.
  + Click Review + Create
* Summary – pre-deployment
  + A screenshot of a computer

    AI-generated content may be incorrect.
  + Click Create
* Post-deployment
  + A screenshot of a computer

    AI-generated content may be incorrect.

## Enable Application Insights

* Go to Application Insights
* Click + Create
* Project Details
  + Subscription - select the correct Subscription
  + Resource group - select the correct resource group
* Instance Details
  + Name – enter a name
  + Region - select the correct region
* Workspace Details
  + Subscription - select the correct Subscription
  + Log Analytics Workspace – select the log analytics workspace created earlier
    - A screenshot of a computer

      AI-generated content may be incorrect.
  + Click Review + create
* Summary – pre-deployment
  + A screenshot of a computer

    AI-generated content may be incorrect.
  + Click Create
* Post-deployment
  + A screenshot of a computer

    AI-generated content may be incorrect.

## Create Storage Account

* Go to Storage accounts
* Click + Create
* Basics
  + Subscription - select the correct Subscription
  + Resource group - select the correct resource group
  + Storage account name – enter a name for the storage account (The field can contain only lowercase letters and numbers. The name must be between 3 and 24 characters. Must be globally unique within all of Azure)
  + Region – select the correct region
  + Primary service – select Azure Blob Storage or Azure Data Lake Storage Gen 2
  + Performance – leave default of Standard
  + Redundancy – select Locally-redundant storage (LRS)
    - A screenshot of a computer

      AI-generated content may be incorrect.
  + All other settings will be left at default
  + Click Review + create
* Summary – pre-deployment
  + A screenshot of a computer

    AI-generated content may be incorrect.
  + A screenshot of a computer screen

    AI-generated content may be incorrect.
  + Click Create
* Post-deployment
  + A screenshot of a computer

    AI-generated content may be incorrect.

## Create Subnet Flow Log

* Go to Network Watcher
* Go to Logs / Flow logs
* Click + Create
* Basics
  + Project details
    - Subscription - select the correct Subscription
    - Flow log type – select Virtual network
    - Click + Select target resource to expand then select Subnet
    - Select AzureFirewallSubnet
      * A screenshot of a chat

        AI-generated content may be incorrect.
  + Click Confirm selection
  + Instance details
    - Subscription - select the correct Subscription
    - Storage accounts – select the storage account created earlier
    - Retention days – (we suggest 1 day)
      * A screenshot of a computer

        AI-generated content may be incorrect.
    - Click Next: Analytics
* Analytics
  + Check the box for Enable traffic analytics
  + Traffic analytics processing interval – select Every 10 mins
  + Subscription - select the correct Subscription
  + Log Analytics Workspace – select the log analytics workspace created earlier
    - A screenshot of a screenshot of a computer

      AI-generated content may be incorrect.
  + Click Review + create
* Summary – pre-deployment
  + A screenshot of a computer

    AI-generated content may be incorrect.
  + Click Create
* Post-deployment
  + A screenshot of a computer

    AI-generated content may be incorrect.

## Create DNS Security Policy

This Azure feature is currently only available in Azure Commercial.

* Go to DNS Security Policies
* Click + Create
* Basics
  + Project details
    - Subscription - select the correct Subscription
    - Resource group - select the correct resource group
  + Instance details
    - Instance name – give it a name
    - Region – select the correct region
    - A screenshot of a computer screen

      AI-generated content may be incorrect.
* Click Next: Virtual Network Link
  + Click + Add
  + Select the virtual network
  + Click Review + create
* Summary – pre-deployment
  + A screenshot of a computer

    AI-generated content may be incorrect.
  + Click Create
* Post-deployment
  + A screenshot of a computer

    AI-generated content may be incorrect.
* Click Go to resource
* Then go to Monitoring / Diagnostic settings
  + A screenshot of a computer

    AI-generated content may be incorrect.
* Click Add diagnostic settings
* For Diagnostic setting name, enter a name
* For Logs / Category groups, select allLogs
* For Destination details, select Stream to an Event Hub and select your environment’s event hub info.
  + A screenshot of a computer

    AI-generated content may be incorrect.
* Click Save

## Additional Configuration

### Configure Log Analytic Export to Event Hub

* Traffic must flow through the firewall for at least one hour or more before this can be configured
* Go to Log Analytics Workspaces
* Click on the name of the log analytics workspaces you created earlier
* Go to Settings / Data export
* Click + New export rule
  + Rule name – give it a name
  + Click Next
  + Source – select table name NTANetAnalytics (if not there, you may need to wait longer for the table to be created)
    - A screenshot of a computer

      AI-generated content may be incorrect.
  + Click Next
  + Destination type – select Event Hub
  + Subscription - select the correct Subscription
  + Event Hub Namespace - select the event hub namespace created earlier
  + Event Hub Name - select the event hub name created earlier
    - A screenshot of a computer

      AI-generated content may be incorrect.
  + Click Next
* Summary – pre-deployment
  + A screenshot of a computer

    AI-generated content may be incorrect.
  + Click Create
* Post-deployment
  + A screenshot of a chat

    AI-generated content may be incorrect.

Your environment is now ready for both the Blocklist Integration and/or the Log Forwarding Integration.