

AZURE CLOUD WORKLOAD PROTECTION



*Agent-less discovery for no-scan always on detection
powered by ThreatWorx*

1

CONFIGURING YOUR AZURE ENVIRONMENT

LogAnalytics workspace and Automation account is required to gather inventory for your Azure cloud, ensure both exist as part of your subscription using Azure Portal.

Link the automation account with the LogAnalytics workspace.

The screenshot shows the Azure Portal interface for an Automation Account. The title bar reads "Autmate-Log-418abed9-b812-40d4-9825-72ee6f3d846b | Linked workspace". Below the title bar, there are navigation links: "Go to workspace" and "Unlink workspace". The main content area is divided into two sections: "Linked workspace" and "Unlink workspace".

Linked workspace
This Automation account is linked to the following Log Analytics workspace: [loganalytics-418abed9-b812-40d4-9825-72ee6f3d846b](#)

Unlink workspace
To unlink this Automation account and the Log Analytics workspace you must first remove solutions that have a dependency on Automation from the workspace. These are the following:

- Update Management
- Change Tracking
- Start/Stop VMs during off-hours

After you remove these solutions you can click **Unlink workspace** above to complete the unlinking.

If you use the Update Management solution you optionally may want to remove some items that are no longer needed after you remove the solution.

- Update schedules (will have names that match the names of the update deployments you created) [View schedules](#)
- Hybrid worker groups created for the solution (will have names like machine1.contoso.com_3ceb8108-26c9-4051-b6b3-227600d715c8). [Learn how to remove a hybrid worker group.](#)

2

ENABLE INVENTORY COLLECTION FOR THE AUTOMATION ACCOUNT.

In automation account , select “Configuration Management => Inventory” to enable inventory collection.

**Follow the instructions mentioned here for details,
<https://docs.microsoft.com/en-us/azure/automation/automation-tutorial-installed-software>**

3

CREATE AN AZURE ACTIVE DIRECTORY APP

This app will be used by ThreatWorx to pull inventory information so you can choose to name it as your “ThreatWorx” app.

- Associate the permissions, “Read Logs Analytics Data” and “user_impersonation” to this app.
- Generate a client secret that the app uses to prove its identity

Note, that ThreatWorx as a service does not need access to this app and the credentials of this app remain local to your environment.

All services > App registrations > Test-App

Test-App | API permissions ✎

Search (Cmd+/) Refresh Got feedback?

Overview
Quickstart
Integration assistant

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles | Preview
- Owners
- Roles and administrators | Preview
- Manifest

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for Default Directory

| API / Permissions name | Type | Description | Admin consent req... | Status |
|--------------------------------|-------------|--|----------------------|-------------------------------|
| ▼ Azure Service Management (1) | | | | |
| user_impersonation | Delegated | Access Azure Service Management as organization use... | No | Granted for Default Dire... ✓ |
| ▼ Log Analytics API (1) | | | | |
| Data.Read | Application | Read Log Analytics data | Yes | Granted for Default Dire... ✓ |
| ▼ Microsoft Graph (1) | | | | |
| User.Read | Delegated | Sign in and read user profile | No | Granted for Default Dire... ✓ |

To view and manage permissions and user consent, try [Enterprise applications](#).

All services > App registrations > Test-App

Test-App | Certificates & secrets ✎

Search (Cmd+/) Got feedback?

Overview
Quickstart
Integration assistant

Manage

- Branding
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API
- App roles | Preview
- Owners
- Roles and administrators | Preview
- Manifest

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

| Thumbprint | Start date | Expires | ID |
|---|------------|---------|----|
| No certificates have been added for this application. | | | |

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

| Description | Expires | Value | ID |
|------------------|-----------|----------|----|
| new-secret | 5/18/2021 | Av7***** | |
| inventory-secret | 5/18/2022 | -z***** | |

Support + Troubleshooting

- Troubleshooting
- New support request

4

GRANT ACTIVE DIRECTORY APPLICATION ACCESS TO LOG ANALYTICS WORKSPACE

Select “Access Control (IAM)” after selecting the LogAnalytics workspace. Add the app created in step(3) and give it a “Reader” or “Contributor” role.

LogAnalytics-418abed9-b812-40d4-9825-72ee6f3d846b | Access control (IAM)

Search (Cmd+/) Add Download role assignments Edit columns Refresh Remove Got feedback?

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Settings Locks Agents management Agents configuration Linked storage accounts Network Isolation Advanced settings General Workspace summary Workbooks

Check access Role assignments Roles Deny assignments Classic administrators

Number of role assignments for this subscription 10 2000

Test-App Type: All Role: All Scope: All scopes Group by: Role

Showing a filtered set of results. Total number of role assignments: 10

2 items (2 Service Principals)

| <input type="checkbox"/> | Name | Type | Role | Scope |
|--------------------------|-------------|------|-------------|--------------------------|
| <input type="checkbox"/> | Contributor | | | |
| <input type="checkbox"/> | Test-App | App | Contributor | This resource |
| <input type="checkbox"/> | Reader | | | |
| <input type="checkbox"/> | Test-App | App | Reader | Subscription (Inherited) |

5

ENSURE THAT THE APPLICATION IS ALSO ADDED AS PART OF THE SUBSCRIPTION

Select the Subscription, and Access Control (IAM). Add your application with a “Reader” role

Pay-As-You-Go | Access control (IAM)

Subscription

Search (Cmd+/) Add Download role assignments Edit columns Refresh Remove Got feedback?

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Security Events Cost Management Cost analysis Cost alerts Budgets Advisor recommendations Billing

Check access Role assignments Roles Deny assignments Classic administrators

Number of role assignments for this subscription 10 2000

Test-App Type: All Role: All Scope: All scopes Group by: Role

Showing a filtered set of results. Total number of role assignments: 5

1 items (1 Service Principals)

| <input type="checkbox"/> | Name | Type | Role | Scope |
|--------------------------|----------|------|--------|---------------|
| <input type="checkbox"/> | Reader | | | |
| <input type="checkbox"/> | Test-App | App | Reader | This resource |

6

INVENTORY IN LOG ANALYTICS WORKSPACE

You should now see inventory in the log analytics workspace. Ensure that you are able to see the inventory before moving on to the next steps.

Tip: If you don't see inventory flowing in the log analytics workspace, follow the trouble shooting steps provided in the Azure documentation.

The screenshot shows the Azure Autmate-Log-4 Inventory page. The interface includes a search bar, navigation tabs for 'New software' (0) and 'Machines reporting' (1), and a table of Windows Services. The table has columns for Service, Display Name, Status, Start up type, Last Refreshed Time, and Machines. The 'Machines' column shows a count of 1 for each service.

| Service | Display Name | Status | Start up type | Last Refreshed Time | Machines |
|--------------------------|------------------------------------|---------|---------------|---------------------|----------|
| COMSysApp | COM+ System Application | Stopped | Manual | 2/6/2021, 3:38 PM | 1 |
| CryptSvc | Cryptographic Services | Running | Auto | 2/6/2021, 3:38 PM | 1 |
| DcomLaunch | DCOM Server Process Launcher | Running | Auto | 2/6/2021, 3:38 PM | 1 |
| defragvc | Optimize drives | Stopped | Manual | 2/6/2021, 3:38 PM | 1 |
| DeviceAssociationService | Device Association Service | Stopped | Manual | 2/6/2021, 3:38 PM | 1 |
| DeviceInstall | Device Install Service | Stopped | Manual | 2/6/2021, 3:38 PM | 1 |
| Dhcp | DHCP Client | Running | Auto | 2/6/2021, 3:38 PM | 1 |
| DiagTrack | Diagnostics Tracking Service | Running | Auto | 2/6/2021, 3:38 PM | 1 |
| Dnscache | DNS Client | Running | Auto | 2/6/2021, 3:38 PM | 1 |
| dot3svc | Wired AutoConfig | Stopped | Manual | 2/6/2021, 3:38 PM | 1 |
| DPS | Diagnostic Policy Service | Stopped | Auto | 2/6/2021, 3:38 PM | 1 |
| DismSvc | Device Setup Manager | Running | Manual | 2/6/2021, 3:38 PM | 1 |
| EapHost | Extensible Authentication Protocol | Stopped | Manual | 2/6/2021, 3:38 PM | 1 |
| EFSS | Encrypting File System (EFS) | Stopped | Manual | 2/6/2021, 3:38 PM | 1 |
| EventLog | Windows Event Log | Running | Auto | 2/6/2021, 3:38 PM | 1 |

7

Using the twigs CLI you can now pull the inventory into your ThreatWorx instance (threatworx.io for public SaaS or yourcompany.threatworx.io for dedicated).

```
twigs -v azure --azure_tenant_id "[TENANT_ID]" --
azure_application_id "[APPLICATION_ID]" --
azure_application_key "[APPLICATION_KEY]" --
azure_subscription "[SUBSCRIPTION_ID]" --
azure_resource_group "[RESOURCE_GROUP_NAME]" --
azure_workspace "[LOG_ANALYTICS_WORKSPACE_ID]"
```

Checkout [twigs guide & help videos](https://twigs.threatworx.io/guide) for additional options including CIS benchmark checks for your Azure cloud,
<https://twigs.threatworx.io/guide>

THREATWORX CONSOLE

Analytics, security vulnerabilities, mis-configurations, static and dynamic analysis for base images, running apps and containers can now be managed from the I3 console.



| Date | Title | Rating | Resource | Type | Status |
|--------------|--|----------|---------------|------------------|--------|
| Aug 26, 2020 | 1.3 Ensure that there are no guest users | Critical | Pay-As-You-Go | Misconfiguration | OPEN |
| Aug 26, 2020 | 1.23 Ensure that no custom subscription owner roles are created | Critical | Pay-As-You-Go | Misconfiguration | OPEN |
| Aug 26, 2020 | 2.2 Ensure that 'Automatic provisioning of monitoring agent' is set to 'On' | Critical | Pay-As-You-Go | Misconfiguration | OPEN |
| Aug 26, 2020 | 2.7 Ensure that 'Network security groups' is set to 'On' | Critical | Pay-As-You-Go | Misconfiguration | OPEN |
| Aug 26, 2020 | 2.8 Ensure that 'Web application firewall' is set to 'On' | Critical | Pay-As-You-Go | Misconfiguration | OPEN |
| Aug 26, 2020 | 2.11 Ensure that 'Storage Encryption' is set to 'On' | Critical | Pay-As-You-Go | Misconfiguration | OPEN |
| Aug 26, 2020 | 2.14 Ensure that 'SQL auditing & Threat detection' is set to 'On' | Critical | Pay-As-You-Go | Misconfiguration | OPEN |
| Aug 26, 2020 | 2.15 Ensure that 'SQL Encryption' is set to 'On' | Critical | Pay-As-You-Go | Misconfiguration | OPEN |
| Aug 26, 2020 | 2.17 Ensure that security contact 'Phone number' is set | Critical | Pay-As-You-Go | Misconfiguration | OPEN |
| Aug 26, 2020 | 2.18 Ensure that 'Send me emails about alerts' is set to 'On' | Critical | Pay-As-You-Go | Misconfiguration | OPEN |
| Aug 26, 2020 | 2.19 Ensure that 'Send email also to subscription owners' is set to 'On' | Critical | Pay-As-You-Go | Misconfiguration | OPEN |
| Aug 26, 2020 | 5.1 Ensure that a Log Profile exists | Critical | Pay-As-You-Go | Misconfiguration | OPEN |
| Aug 26, 2020 | 5.2 Ensure that Activity Log Retention is set 365 days or greater | Critical | Pay-As-You-Go | Misconfiguration | OPEN |
| Aug 26, 2020 | 5.3 Ensure that Activity Log Alert exists for Create Policy Assignment | Critical | Pay-As-You-Go | Misconfiguration | OPEN |
| Aug 26, 2020 | 5.4 Ensure that Activity Log Alert exists for Create or Update Network Security Group | Critical | Pay-As-You-Go | Misconfiguration | OPEN |
| Aug 26, 2020 | 5.5 Ensure that Activity Log Alert exists for Delete Network Security Group | Critical | Pay-As-You-Go | Misconfiguration | OPEN |
| Aug 26, 2020 | 5.6 Ensure that Activity Log Alert exists for Create or Update Network Security Group Rule | Critical | Pay-As-You-Go | Misconfiguration | OPEN |

| | Risk Score | Recorded On | CVE / Advisory | Affected Product | Rating | Priority | Status |
|------|------------|--------------|----------------|--------------------------------|----------|----------|--------|
| 🚩🚩🚩 | 80 | Nov 28, 2020 | CVE-2018-8453 | Windows Server 2019 Datacenter | Critical | Now | OPEN |
| 🚩🚩 | 80 | Nov 28, 2020 | CVE-2019-0859 | Windows Server 2019 Datacenter | Critical | Now | OPEN |
| 🚩🚩🚩 | 80 | Nov 28, 2020 | CVE-2019-0803 | Windows Server 2019 Datacenter | Critical | Now | OPEN |
| 🚩🚩 | 80 | Nov 28, 2020 | CVE-2019-0703 | Windows Server 2019 Datacenter | Medium | Now | OPEN |
| 🚩🚩🚩🚩 | 80 | Nov 28, 2020 | CVE-2020-0601 | Windows Server 2019 Datacenter | Severe | Now | OPEN |
| 🚩🚩🚩 | 80 | Nov 28, 2020 | CVE-2020-0787 | Windows Server 2019 Datacenter | Critical | Now | OPEN |
| 🚩🚩🚩 | 80 | Nov 28, 2020 | CVE-2020-1054 | Windows Server 2019 Datacenter | Critical | Now | OPEN |
| 🚩🚩🚩 | 80 | Nov 28, 2020 | CVE-2020-0986 | Windows Server 2019 Datacenter | Critical | Now | OPEN |
| 🚩🚩🚩 | 80 | Nov 28, 2020 | CVE-2020-1350 | Windows Server 2019 Datacenter | Urgent | Now | OPEN |
| 🚩🚩🚩🚩 | 80 | Nov 28, 2020 | CVE-2020-1472 | Windows Server 2019 Datacenter | Urgent | Now | OPEN |
| 🚩🚩 | 75 | Nov 28, 2020 | CVE-2018-8637 | Windows Server 2019 Datacenter | Medium | Now | OPEN |
| 🚩🚩 | 75 | Nov 28, 2020 | CVE-2018-8638 | Windows Server 2019 Datacenter | Medium | Now | OPEN |
| 🚩🚩 | 75 | Nov 28, 2020 | CVE-2018-8641 | Windows Server 2019 Datacenter | Critical | Now | OPEN |
| 🚩🚩 | 75 | Nov 28, 2020 | CVE-2018-8477 | Windows Server 2019 Datacenter | Medium | Now | OPEN |
| 🚩🚩 | 75 | Nov 28, 2020 | CVE-2018-8514 | Windows Server 2019 Datacenter | Medium | Now | OPEN |
| 🚩🚩 | 75 | Nov 28, 2020 | CVE-2018-8596 | Windows Server 2019 Datacenter | Severe | Now | OPEN |
| 🚩🚩 | 75 | Nov 28, 2020 | CVE-2018-8595 | Windows Server 2019 Datacenter | Severe | Now | OPEN |
| 🚩🚩 | 75 | Nov 28, 2020 | CVE-2019-1040 | Windows Server 2019 Datacenter | Severe | Now | OPEN |