

Integration with Dynatrace (APM)

- [Configure Dynatrace APM Integration](#)
- [Deploy Dynatrace](#)
- [Configure Dynatrace Integration for AIQ Monitoring](#)

Configure Dynatrace APM Integration

Last reviewed: September 24, 2026

Use this article when AIQ executions need to be reviewed alongside Dynatrace service, application, or synthetic monitoring data.

What changed in this article

- Confirm the Dynatrace tenant URL, API token scope, monitored entity, and management zone before saving the integration.
- Use read-only API access where possible and avoid embedding tokens in article text or screenshots.
- Validate with a small execution so the AIQ run name and Dynatrace time range can be matched cleanly.

Validation workflow

1. Get the tenant URL and token requirements from the Dynatrace administrator.
2. Map the AIQ execution to the correct Dynatrace entity or service.
3. Run a validation scenario and confirm Dynatrace metrics line up with AIQ start and end times.

Review note: Updated the page to focus on Dynatrace tenant/entity mapping rather than generic APM setup.

Last updated: September 24, 2026

If you have feedback on this topic, contact documentation@appvance.ai.

Deploy Dynatrace

A single Dynatrace OneAgent monitors real user experience and the technologies, services, and applications running in your environment. Install OneAgent on each host that contains processes you want to monitor.

Install the Dynatrace OneAgent on Windows

1. Sign in to your Dynatrace account and open **Deploy Dynatrace** from the left navigation panel.
2. Select **Start Installation**.
3. Select **Windows** as the target platform.
4. Download and run the installer on the target host using the download link provided by Dynatrace.
5. Restart the processes that you want to monitor.

Install the Dynatrace OneAgent on Linux

The supplied installer targets Linux x86/64. Run the installation script on each Linux machine that you want to monitor.

On the target host, download the installer:

```
wget -O Dynatrace-OneAgent-Linux-1.141.205.sh "Your OneAgent URL"
```

Verify the installer signature. Download the Dynatrace root certificate from

<https://ca.dynatrace.com/dt-root.cert.pem>, then run:

```
wget https://ca.dynatrace.com/dt-root.cert.pem ; ( echo 'Content-Type: multipart/signed;  
protocol="application/x-pkcs7-signature"; micalg="sha-256"; boundary="--SIGNED-INSTALLER"';  
echo ; echo ; echo '----SIGNED-INSTALLER' ; cat Dynatrace-OneAgent-Linux-1.141.205.sh ) |
```

```
openssl cms -verify -CAfile dt-root.cert.pem > /dev/null
```

Run the installer with root rights:

```
/bin/sh Dynatrace-OneAgent-Linux-1.141.205.sh APP_LOG_CONTENT_ACCESS=1
```

Restart the processes that you want to monitor.

Last updated: October 15, 2026

If you have feedback on this topic, contact documentation@appvance.ai.

Configure Dynatrace Integration for AIQ Monitoring

Configure Dynatrace Integration for AIQ Monitoring

Last reviewed: September 21, 2026

Use this page when AIQ test results need to be correlated with Dynatrace metrics and traces. Coordinate tenant access with the monitoring owner.

When to use this guidance

- Dynatrace monitors the system under test.
- AIQ performance results need APM context.
- You need to validate token scope, entity selection, and time correlation.

Recommended approach

1. Confirm the Dynatrace tenant URL and target entities or management zones.
2. Create an approved API token with the minimum required read scope.
3. Configure AIQ with the Dynatrace endpoint and token according to the current version.
4. Run a short AIQ test and compare the execution time window with Dynatrace data.
5. Use consistent tags or test names to make executions easy to find.

Note: Protect Dynatrace tokens as secrets and rotate them according to policy.

Last updated: September 21, 2026

If you have feedback on this topic, contact documentation@appvance.ai.