IoT Hub Device Provisioning Service concepts

IoT Hub Device Provisioning Service is a helper service for IoT Hub that you use to configure zero-touch device provisioning to a specified IoT hub. With the Device Provisioning Service, you can auto-provision millions of devices in a secure and scalable manner.

Device provisioning is a two part process. The first part is establishing the initial connection between the device and the IoT solution by *registering* the device. The second part is applying the proper *configuration* to the device based on the specific requirements of the solution. Once both steps have been completed, the device has been fully *provisioned*. Device Provisioning Service automates both steps to provide a seamless provisioning experience for the device.

This article gives an overview of the provisioning concepts most applicable to managing the *service*. This article is most relevant to personas involved in the cloud setup step of getting a device ready for deployment.

Service operations endpoint

The service operations endpoint is the endpoint for managing the service settings and maintaining the enrollment list. This endpoint is only used by the service administrator; it is not used by devices.

Device provisioning endpoint

The device provisioning endpoint is the single endpoint all devices use for auto-provisioning. The URL is the same for all provisioning service instances, to eliminate the need to reflash devices with new connection information in supply chain scenarios. The ID scope ensures tenant isolation.

Linked IoT hubs

The Device Provisioning Service can only provision devices to IoT hubs that have been linked to it. Linking an IoT hub to an instance of the Device Provisioning service gives the service read/write permissions to the IoT hub's device registry; with the link, a Device Provisioning service can register a device ID and set the initial configuration in the device twin. Linked IoT hubs may be in any Azure region. You may link hubs in other subscriptions to your provisioning service.

Allocation policy

The service-level setting that determines how Device Provisioning Service assigns devices to an IoT hub. There are three supported allocation policies:

- **Evenly weighted distribution**: linked IoT hubs are equally likely to have devices provisioned to them. The default setting. If you are provisioning devices to only one IoT hub, you can keep this setting.
- **Lowest latency**: devices are provisioned to an IoT hub with the lowest latency to the device. If multiple linked IoT hubs would provide the same lowest latency, the provisioning service hashes devices across those hubs
- **Static configuration via the enrollment list**: specification of the desired IoT hub in the enrollment list takes priority over the service-level allocation policy.

Enrollment

An enrollment is the record of devices or groups of devices that may register through auto-provisioning. The enrollment record contains information about the device or group of devices, including:

- the attestation mechanism used by the device
- the optional initial desired configuration
- desired IoT hub
- the desired device ID

There are two types of enrollments supported by Device Provisioning Service:

Enrollment group

An enrollment group is a group of devices that share a specific attestation mechanism. Enrollment groups support both X.509 as well as symmetric. All devices in the X.509 enrollment group present X.509 certificates that have been signed by the same root or intermediate Certificate Authority (CA). Each device in the symmetric key enrollment group present SAS tokens derived from the group symmetric key. The enrollment group name and certificate name must be alphanumeric, lowercase, and may contain hyphens.

> [!TIP] We recommend using an enrollment group for a large number of devices that share a desired initial configuration, or for devices all going to the same tenant.

Individual enrollment

An individual enrollment is an entry for a single device that may register. Individual enrollments may use either X.509 leaf certificates or SAS tokens (from a physical or virtual TPM) as attestation mechanisms. The registration ID in an individual enrollment is alphanumeric, lowercase, and may contain hyphens. Individual enrollments may have the desired IoT hub device ID specified.

> [!TIP] We recommend using individual enrollments for devices that require unique initial configurations, or for devices that can only authenticate using SAS tokens via TPM attestation.

Registration

A registration is the record of a device successfully registering/provisioning to an IoT Hub via the Device Provisioning Service. Registration records are created automatically; they can be deleted, but they cannot be updated.

Operations

Operations are the billing unit of the Device Provisioning Service. One operation is the successful completion of one instruction to the service. Operations include device registrations and re-registrations; operations also include service-side changes such as adding enrollment list entries, and updating enrollment list entries.