

Connect services manage, update, remotely monitor, collect, and store data from smart devices ranging from consumer wearables to large medical-grade systems, both Philips and third-party.

Value

- **Device management:** Highly scalable and secure services to manage connected devices for remote service, diagnostics, software updates, messaging, and device control
- **Collect health and wellness data:** Collect, store, validate, correlate, and broker both personal (health) measurements and observations, as well as device data
- **Secure cloud connectivity:** Secure Internet connectivity between installed bases and the cloud, even in constrained environments like hospitals. Connect your devices with your cloud services using certificates, a single domain name, static IP address, or Customer Managed VPN (CMVPN), and have your data encrypted both in transit as well as at rest.

Features

- **The Provisioning** service allows you to securely register devices and mobile apps when you first connect them. As a result, devices and apps obtain their unique identities, keys, and certificates dynamically 'over-the-air,' eliminating the need to provision them with a unique identity up-front in the factory. All consuming clients – users, services, and devices – require this unique identity and key to use HSDP services.
- **The Firmware** service enables clients to update firmware or software for their devices 'over-the-air'. This allows you to update your installed base with new features or fixes using a flexible rule-based mechanism that helps you identify target groups.
- **The IoT Gateway** service enables devices to connect securely (using an access token or certificate) into the IoT message bus and start communicating with other IoT services or devices using the MQTT protocol and "publish/subscribe" pattern.
- **The Profile** service implements a "Shadow and Digital Twin" concept, which is a virtual representation of the device state. A Device Profile can make the device's state, status, and properties available to applications and other services even when the device is disconnected.
- **The Control** service is a highly scalable messaging service that allows devices and applications to exchange events and messages. You can also use it to control devices remotely using the MQTT or HTTPS protocol to send and receive messages even when devices are temporarily disconnected.
- **The Data Broker** service allows devices and applications to send data and have it distributed (brokered) to configured repositories or API endpoints. Devices and apps can publish the data over the MQTT protocol or use the REST APIs to send the data over HTTPS. Based on customer configuration, the Data Broker service distributes the data to one or more destinations. This can include customer endpoints, as well as data repositories that are part of HSDP-Store services.
- **The Pairing** service enables you to pair devices with users or patients and create virtual ecosystems in which you can securely share data and remotely control devices.
- **The Tunnel** service offers point-to-point secure VPN sessions, enabling you to remotely connect to the device even when it is behind a firewall.
- **The Concentrator** service provides secure connectivity from on premises to the cloud using a static IP address and a single domain name to ease your site's outgoing traffic configuration. It also integrates with CMVPN and enables you to route device traffic over the VPN to your cloud services under the same single IP address and domain name.

For more information,
please go to hsdp.io.