(intel)

# Zero-Touch Provisioning for Edge Devices and Software-Defined Networks

**The Intel® Secure Device Onboard (Intel® SDO) service helps end-customers, networking software vendors and device manufacturers interconnect in an end-to-end IoT ecosystem, in seconds. Using automatic, "zero-touch" provisioning.**

## Key Capabilities

- **Vendor Agnostic Provisioning.** Ability to provision any device (Intel or ARM hardware) to any vendor's DMS system.

- **Provision Edge Services.** Ability to provision "white box" universal customer premises equipment (uCPE), with virtual networking functions (VNFs).

- **Edge Security.** Securely register devices and dynamically deploy edge perimeter defenses as devices are powered up.

- **Supply Chain Savings.** Dramatic savings for the device supply chain, because vendors can build and drop-ship standard-image devices that get customized via provisioning in the field.

## Driving Scalable Deployments Across the Edge

The IoT industry is now making rapid progress. New computing paradigms have given rise to Edge Computing as fundamental architecture of IoT deployments. Workload processing has advanced to distribute storage, compute and analytics more efficiently. Virtualization of network functions is possible using commercial-off-the-shelf hardware. Yet the inability to provision edge devices and servers in a secure and automated fashion, quickly and easily, has significantly slowed IoT adoption, and also led to deployments with security vulnerabilities.

A typical IoT implementation requires customers to connect a wide variety of devices to a device management system (DMS), which runs either on-premise or in the cloud. DMS systems are managed by operational technology (OT), and interface with information technology (IT). Together, these technologies manage device security, access control, networking and communications, and IoT analytics. (see Figure 1). All components must be deployed together for an IoT deployment to begin processing data that derives value for the business.

Intel SDO is an IoT device onboarding service that delivers open, consistent provisioning across an IoT and Enterprise edge. It automates DMS device registration, and when combined with Intel's optimized hardware networking and hardware-enhanced security, puts the many benefits of secure edge computing within easy reach.
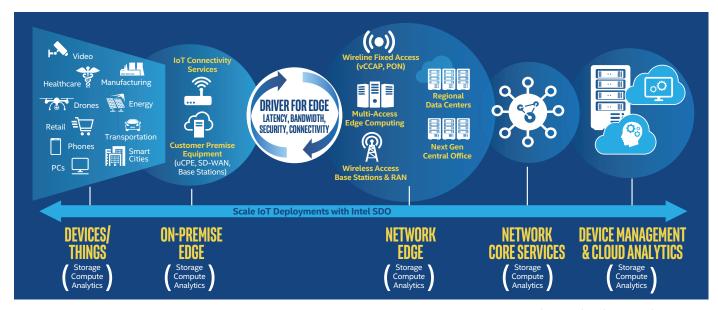


**Figure 1.** Edge to Cloud IoT Deployment

## Zero-Touch, Late-Binding Provisioning for IoT Devices

Most "zero-touch" provisioning solutions in the market today require a unique device SKU for each customer/cloud combination. This adds significant friction to the supply chain because unique devices are needed for each end-customer—requiring that products be built-to-order. Intel SDO uses a "late binding" approach, however, that makes it possible to configure devices at the point of installation, rather than having to be customized in advance for each customer system. This capability not only improves ease of installation, but also enables original device manufacturers (ODMs) to build identical IoT devices in high volume.
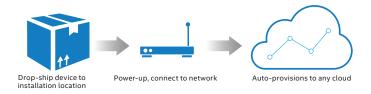
Drop-ship device to installation location → Power-up, connect to network → Auto-provisions to any cloud

**Figure 2:** Intel SDO Streamlined Use Case

Intel SDO is implemented across an IoT solution ecosystem using software-enabling toolkits to configure devices, DMS systems, and services to run the appropriate onboarding protocols. This Intel SDO enablement model can be applied to sensors, devices, and IoT edge servers. The payload delivered to each device is configurable, able to address various use cases and IT security requirements. Typical payloads that can be sent to the device include an operational device identity, a DMS agent, and software updates.

## The Software Defined On-Premise Edge

Software defined, wide area networks (SD-WAN) enable automated, centralized provisioning of virtual private connections between enterprise branch offices—including remote offices, factories, retail outlets, hospitals, and data centers. SD-WAN endpoints and controllers can be implemented as a virtualized network function (VNF) run on 'white box', commercial off-the-shelf (COTS) servers located at the enterprise branch, enterprise datacenter, and in gateways in a private or public cloud. As such, SD-WAN has become the primary use case for edge servers, more commonly known as universal customer premises equipment (uCPE). Due to an emerging need for security at each branch office, virtual firewalls are emerging as vital use case for uCPE.

## Provisioning Virtualized Networking Services: Art of the Possible

Intel SDO can be used to simplify the uCPE provisioning process, while also proving increased levels of security. Figure 3 illustrates the enablement workflow:

- **Step 1**: The bare metal Intel edge server is mass produced as a single SKU with a standard image, hardware root of trust and Intel SDO agent.

- **Step 2**: The enterprise customer orders a uCPE and one or more virtual networking functions from a communication service provider (CoSP). An "ownership credential" is loaded into the Service Chain Orchestration Console and Intel SDO Rendezvous Service as part of a sales order, and the bare metal device is drop-shipped to the install location.
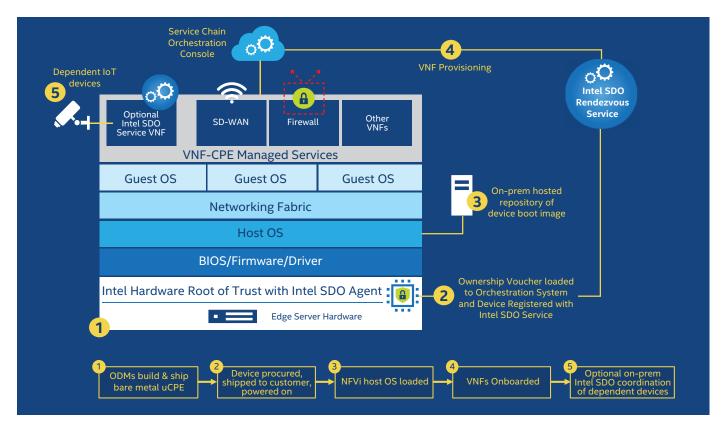
**Figure 3.** Provisioning the uCPE Networking Stack

- **Step 3-4**: At power on, the uCPE, NFVi OS, and SD-WAN, virtual firewall, and other VNFs are automatically and securely onboarded using Intel SDO Rendezvous server, hosted in the cloud.

- **Step 5**: Optionally, the Intel SDO service can be run on the uCPE as a VNF to onboard dependent IoT devices from a local edge server rather than a hosted cloud service.

## Use Case: Deploying Edge Computing and IoT for Retail

In a retail IoT deployment, a business and its system integrator must deploy a uCPE supporting SD-WAN, a virtual firewall, and other retail-oriented services, as well as a wide variety of IoT devices. These can include video surveillance sensors, digital advertising smart signage, magic mirrors, and point-of-sale machines that interface with inventory systems.

Without the open onboarding methods offered by Intel SDO, the business must work with its device suppliers to pre-load configurations that work with their DMS or configure devices in the field in ways that are less than optimal from a security perspective. Most deployment plans do not account for the difficulties and timeline extensions required for provisioning. Delays and difficulties in provisioning can dramatically roll back the scope of uCPE and IoT device deployments.

As shown in Figure 4 , a retail business can onboard devices directly to DMS systems that resides in the cloud. With bare metal devices enabled for Intel SDO, a retail installer can merely unbox the devices and use the Intel SDO Installer Tools to get everything up and running. Prior to onboarding, the DMS administrator configures different provisioning payloads and security updates for each device type. After power on, the devices appear configured and live in the DMS console in about 20 seconds, awaiting command-and-control instructions.

## An Open Approach

Intel pioneered its Intel SDO solution to help accelerate IoT deployments. After launching Intel SDO in 2017, Intel collaborated with Arm to deliver a singular method that could provision both the Intel- and Arm-based devices that make up the majority of IoT deployments. In 2019, the use cases and protocols have been submitted to the FIDO Alliance Working Group for IoT to establish a single standards specification. In parallel, Intel and partners are working to release open source software in early 2020.

## Ecosystem Software Solutions Optimized for Accelerated Intel Performance

Intel enables the uCPE ecosystem and the integration of uCPE and the enterprise IoT edge, as shown in Figure 5.

1. Intel enables ODM and OEM partners with processors that scale from Intel Atom®-based SoCs to Intel® Xeon-D-based SoCs to our top of the line Intel Xeon Scalable Processors. Technology performance optimizations include DPDK, Quick Assist, Hyperscan and others.

2. Intel partners with NFVi OS vendors that deliver virtualized uCPE implementations on white box servers.

3. Intel works with NFVi OS and ISV partners to enable SD-WAN, virtual firewalls, and orchestrated service chaining of these workloads.

4. Intel is prototyping new uCPE workloads including predictive and preventative network security analytics, computer vision using AI, and machine learning in partnership with Splunk. Intel is also leveraging the OpenVINO™ toolkit for computer vision.

5. For the enterprise IoT edge, Intel is incorporating Intel SDO into the uCPE for automatic and secure onboarding of attached IoT devices, and for the uCPE itself.
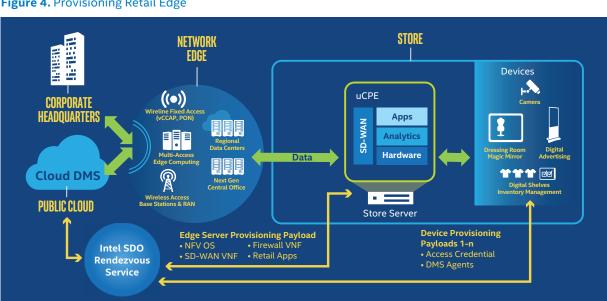
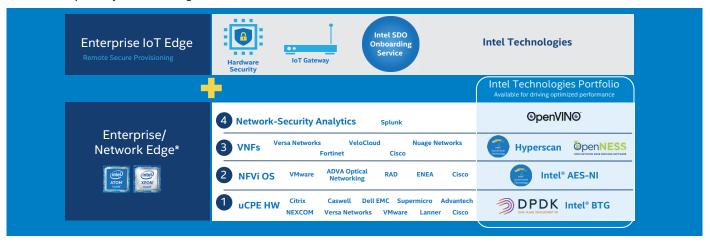**Figure 4.** Provisioning Retail Edge

**Figure 5.** Intel Edge Server Reference Architecture

### Real World Deployment: Zero-Touch Orchestration (ZTO) on Digital Business Marketplace (DBM) – British Telecom

As the world's first end to end deployment of plug and play multi-party secure supply chain (ZTO/DBM), British Telecom's Applied Research recently leveraged Intel SDO to provision and deploy its smart-x solutions in the Adastral Park (AP), home to BT's innovation labs and Innovation Martlesham, an established and growing cluster of over 100 high-tech ICT companies.

This includes various IoT verticals such as smart parking, air quality, edge computing and network virtualization. As part of this deployment, cameras are deployed at AP that utilize artificial intelligence at the edge, to count free carpark spaces, and monitor pedestrian traffic.

This deployment achieved a significant reduction in time and costs while improving end to end security from device to cloud. The DBM concept recently won the Outstanding Catalyst Innovation Award at the TM Forum Digital Transformation World 2019 conference.

## Conclusion

Businesses and their system integrator contractors should not underestimate the time and cost to activate devices and edge servers on the corporate IoT network. An interoperable onboarding model based on industry standards can dramatically increase the number of devices that can be put into service. In addition, use of a consistent hardware-enhanced security model enables security protections that meet IT risk and audit requirements. Secure onboarding based on Intel SDO not only saves time, it also accelerates installation and optimizes the performance benefits of edge computing.

### Learn More on Intel SDO:

1. See demo or gain overview: Visit www.intel.com/securedeviceonboard

2. To gain access to the Intel SDO software and documentation (https://software.intel.com/en-us/secure-device-onboard):

    a. Register for an Intel® Developer Zone (Intel® DZ) account

    b. Request access to Intel SDO Materials

3. Intel SDO Program-Business

    c. Contact Iotonboarding@intel.com for a discussion.

### Learn More on Intel® Select Solutions for uCPE:

https://builders.intel.com/intelselectsolutions/intelselectsolutionsforucpe