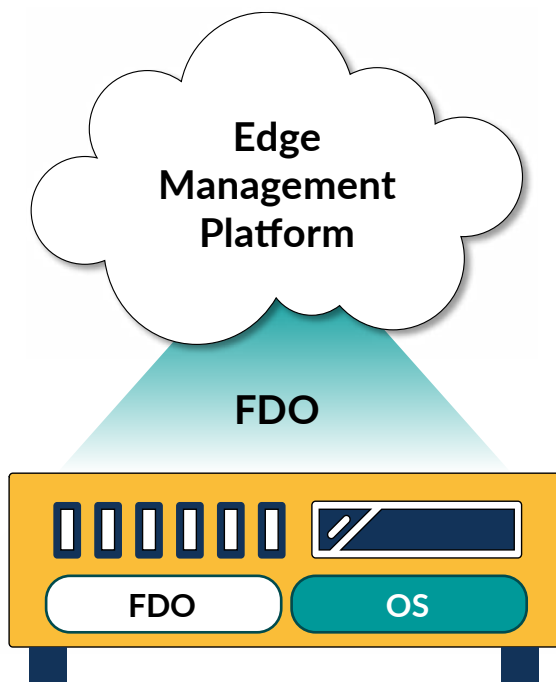


FIDO Bare Metal Onboarding

Extending FIDO to late-bind a device's complete software stack

The FIDO Device Onboard (FDO) specification offers an automatic onboarding protocol for edge nodes, data center servers and IoT devices. This protocol facilitates secure installation of secrets and configuration data into devices to allow for seamless connection to cloud and edge management platforms.

Key benefits of FDO include scalable passwordless authentication, zero-touch onboarding, and zero-trust security, combined with late binding. Late binding allows devices to be manufactured without first identifying the end customer or management platform that they will eventually connect to.



FIDO in an Edge application

FDO is a method to connect a Device to its Management platform

- OS, FDO Client and Application software are installed at Manufacture (or second touch)
- FDO provides Zero-Touch onboarding and Secure Credentialing
- After onboarding, Device and Management platform can interoperate

As FDO is compatible with a wide variety of processors and operating systems, it has broad application across industries such as industrial automation, healthcare, retail, and enterprise. Companies such as Dell, Microsoft, ExxonMobil, and Red Hat have already embraced this technology.

Extending the late binding concept

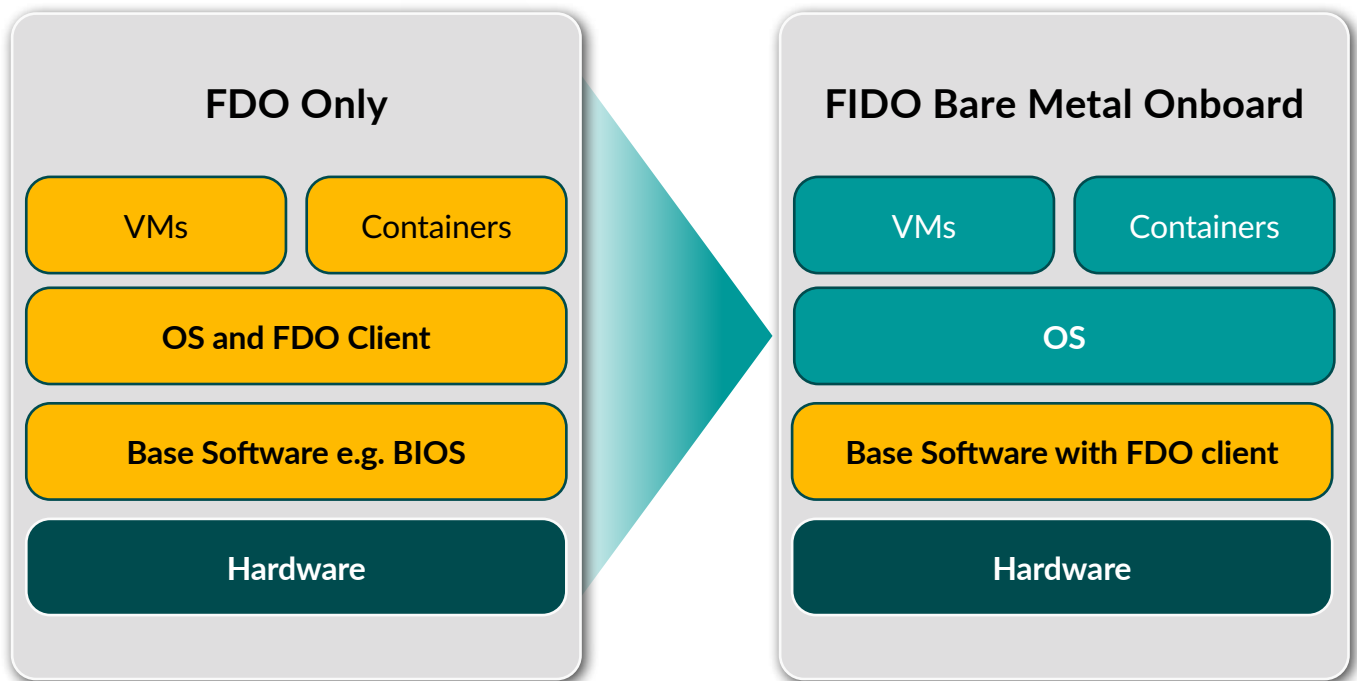
Edge computing is increasingly shifting toward general-purpose edge devices that can run any OS/ software, and often ship without pre-installed application-specific software. In support of this transition, users want to expand the “late binding” of FDO so that it can support the dynamic installation of the entire software stack (OS and applications), not just ownership. FIDO’s Bare Metal Onboarding concept has been created to specifically address this need.

The Unmet Promise of Bare Metal Onboarding

The idea of **bare metal onboarding** isn't new. Most hardware comes with some form of remote management, such as **BMCs (Baseboard Management Controllers)** or **Dell's iDRAC**, while methods like **PXE boot** and **HTTP boot** enable network-based deployment. Operating systems also offer various tools, from **Kickstart files** to **cloud-init**, for automated installation.

However, despite these existing solutions, the journey toward truly automated, secure, and standardized bare metal onboarding has been fraught with challenges, particularly when moving beyond traditional IT environments to the dynamic world of edge computing.

FDO VS FIDO Bare Metal Onboard



Key:



Installed at manufacture (or second touch)



Installed via dynamic late binding

THE HURDLES:

Lack of Zero-Touch, Security Gaps, and Little Standardization

The current landscape of bare metal onboarding falls short in three critical areas:

Limited Automation and Zero-Touch Capabilities:

Many existing methods demand significant manual intervention, such as physically inserting USB devices, tweaking BIOS settings, or relying on an IT person to be hands-on with the hardware. These approaches are fine for traditional data centers where IT staff are inherently trusted and skilled but they cannot support zero-touch scenarios. This is especially true at the edge, where devices might be deployed in remote, unstaffed locations by individuals who aren't IT experts. The vision of simply powering on a device and having it automatically configure itself remains largely unfulfilled.

Inadequate Security for Untrusted Environments:

When an IT professional performs an installation, their knowledge and authorization are implicit. However, in edge computing, operational personnel might lack that expertise or authorization. Relying on models like PXE, which inherently trust the network, poses risks when devices are deployed in potentially untrustworthy environments. A secure bare metal onboarding solution needs to ensure that only authorized software is installed, even when physical access is limited or the local network cannot be fully trusted.

Pervasive Lack of Standardization:

Perhaps the biggest impediment is the lack of industry standardization. There's a dizzying array of proprietary solutions and disparate methods across both hardware and software. Every hardware vendor has its own remote management tools, and nearly every operating system has its own way of handling automated installations. Some methods work only with specific hardware, others are limited to virtual machines, and many have unique requirements. This fragmentation makes it very difficult to create a unified, scalable, and predictable bare metal onboarding process that is both automated and secure across diverse hardware and software ecosystems. Without common standards, achieving true zero-touch and secure deployment at scale remains an elusive goal.

Why the FIDO Device Onboarding Working Group?

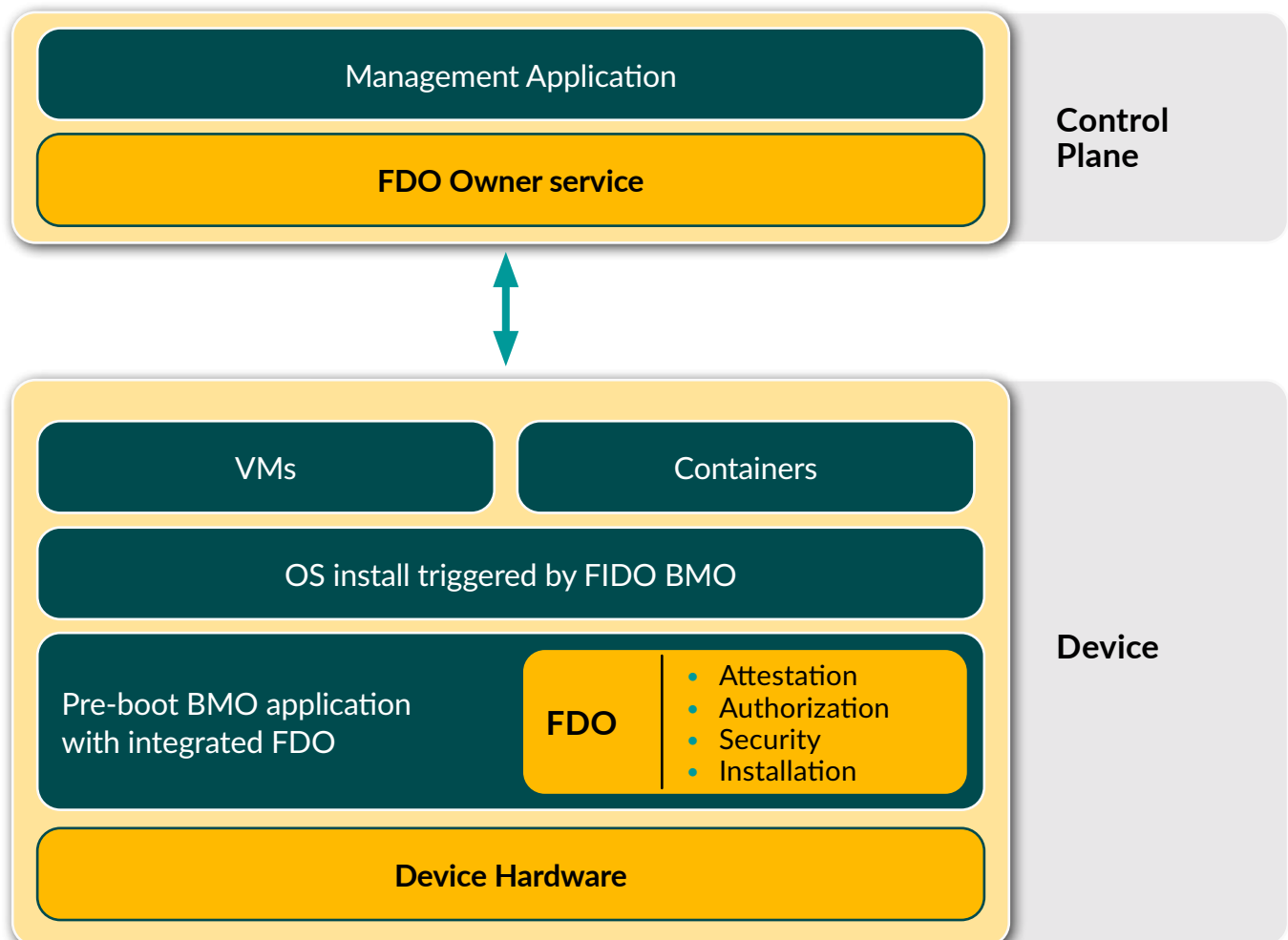
The FIDO Device Onboarding working group is uniquely positioned to address this industry challenge by leveraging FDO's strengths in provable trust and extending its "late-bound" capabilities to software provisioning for general-purpose edge devices, thus creating a truly secure, automated, and standardized solution.

Where does FDO fit in to a FIDO BMO Solution?

FIDO BMO provides dynamic late binding of the OS and Applications software at the time of onboarding to the Management control plane.

FDO provides the key elements for secure remote control:

- Attestation
- Authorization
- Security
- Encrypted channel for delivering commands to the Device



FIDO BMO value proposition

The FIDO BMO concept will enable edge and general-purpose computers to be delivered to end users without predefined knowledge of their operating system or application, offering:

- Late binding of the entire system state
- Compatibility with almost all devices and vendors
- A standardized approach that supports a multitude of commercial off-the-shelf operating systems
- Ability to deliver the base OS and other software components and credentials
- Cryptographic end-to-end assurance: FIDO establishes ownership, FIDO BMO mandates that the system be installed according to the owner's specification
- User-specific configuration options
- Consistent and deterministic outcome
- Additionally, FIDO BMO can unify Known Good State status and version upgrades by supporting:
 - State saving (local or remote)
 - System reinstallation with a new version
 - State restoration post-upgrade

Industry collaboration and standardization

The FIDO Device Onboarding Technical Working Group welcomes feedback on the topics covered in this document and is actively seeking collaboration with industry stakeholders to tackle the challenges of dynamic, late-bound configuration. Interested parties are encouraged to engage with the FIDO Alliance and its members.

FIDO Alliance members can learn more about new FIDO standards and have the opportunity to influence how these standards evolve. Additionally, members can engage with a broad range of thought leaders from leading companies within the broader ecosystem.

Get involved

- ➡ To get involved visit <https://fidoalliance.org/members/become-a-member>
or
- ➡ Use the Contact Us form at <https://fidoalliance.org/contact>