



D9 - Mastering Mender

Secure and Automated Updates for Embedded Linux

Objectives

- Understand the challenges of updating embedded Linux devices
- Automate the update process for embedded Linux devices using Mender
- Set up and configure a Mender server
- Deploy updates to devices using Mender, and monitor their progress.
- Use advanced Mender features such as rollback, A/B updates, and update channels to improve update reliability and flexibility.
- Integrate Mender with cloud providers such as AWS and Azure for OTA updates, and use delta updates to reduce update sizes and bandwidth usage.

Labs are conducted on target boards, that can be:

Dual Cortex/A7-based "STM32MP15-DISCO" boards from STMicroelectronics.

Quad Cortex/A9-based "SabreLite" boards from NXP.

Quad Cortex/A53-based "imx8q-evk" boards from NXP.

Course environment

- Printed course material (in English)
- One Linux PC for two trainees.
- One target platform for two trainees

Prerequisite

- Embedded Linux Build (see our [D1 - Embedded Linux with Buildroot and Yocto](#) course)
- Building a Linux Embedded image using Yocto (see our [Y1 - Yocto Project Development](#) course)
- Preferably knowledge of Advanced Yocto Project usage and adaptation (see our [Y2 - Yocto Project Expert](#) course)

Target Audience

- Any embedded systems engineer or technician with the above prerequisites.

Course Outline

First DAY

Introduction to the update process using Mender

- Overview of the challenges of updating embedded devices
- Update options
 - Locally
 - Remotely
 - Over-the-air (OTA)
- Update risks
- Benefits of using Mender
- Introduction to the Mender architecture
- Mender update strategies
- How mender fits into the overall update process

What to update

- Identifying what needs to be updated on your devices
- Local updates vs OTA updates
- Robust system updates
- Application updates
- Proxy deployments

Mender server

- Installing and configuring a Mender server
- Setting up a Mender server and integrating it with your build system
- Connecting Mender to your build system and creating update artifacts
- Signing update artifacts for security

Exercise: Setting up a Mender server

Deploying updates to devices

- Deploying updates to devices
- Deploy an application update
- Deploy a system update
- Deploy a container update

Exercise: Deploying an update to a device using Mender

Mender artifacts

- The concept of Mender artifacts
- The role of artifacts in the update process
- The different types of artifacts
- Create an update Artifact

Exercise: Create and use artifacts

Second DAY

Advanced Mender features

- Using rollback to revert to a previous version if an update fails
- Implementing A/B updates to minimize downtime during updates
- Managing multiple update channels for different groups of devices
- Making updates robust and secure

Exercise: Rollback to revert to a previous version

Delta updates and the integration with cloud providers

- Introduction to delta updates
- Reduce update sizes and bandwidth usage
- Integrating Mender with AWS and Azure for OTA updates

Exercise: Update device OTA using AWS

Monitoring the update process and troubleshooting issues

- Understanding Mender's logging
- Mender's built-in monitoring capabilities
- Deployment status reports
- Debugging update issues and identifying root causes
- Test updates before deploying

Exercise: Debug and monitor update

Customizing Mender for your specific use case

- Extending Mender with custom scripts and plugins
- Integrating Mender with your existing deployment tools and processes
- Best practices for optimizing the Mender update process for your environment

Exercise: Extending Mender with custom scripts

Securing the update

- Best practices for securing the update process
- Security considerations for remote management
- Ensuring the integrity and authenticity of update artifacts
- Protecting against attacks on the update process
- Tips for hardening your Mender deployment against threats