# DIAL

The Device Interaction and Automation Layer handles multi-vendor device interaction, semantic translation, normalization, and deterministic validation through CLI and API interfaces.




## An integration is a continuing maintenance commitment.

A device integration is not finished when its first process runs. New operating-system releases, command behavior, output formats, and APIs create ongoing maintenance work. As coverage expands, that obligation can consume the capacity intended for the next business outcome. DIAL makes the supported device interaction layer a maintained Gluware capability.

CORE FUNCTIONALITY

### Read across vendors and platforms

Abstract device interaction to retrieve configuration and operational state from supported infrastructure. Applications use the shared layer instead of separate device-handling scripts.

### Translate and render changes

Turn normalized automation into vendor- and platform-specific write operations through CLI or API interfaces.

### Validate against the target

Apply deterministic, model-aware validation and translation for the infrastructure being managed. The same foundation supports intent-based operations and validation of proposed AI actions.

> **Business contribution**
>
> DIAL offloads work that every automation initiative needs but that is not custom to the business. Teams can invest in the policies and processes that reduce exposure, maintain controls, protect services, and support expansion. The maintained foundation reflects more than twelve years and over a million engineering hours of investment, with dozens of DIAL package releases each year.

# DIAL

Functions, dependencies, and operating boundaries.

## RELATED FUNCTIONS AND OPERATING SCOPE

### Device Manager: fleet discovery

Discover and inventory devices, inspect configuration and software state, and maintain the fleet information that network automation depends on.

### Config Model Editor: configuration intent

Model multi-vendor CLI and API intended configuration state with declarative enforcement.

### Titan MCP: supported action validation

Connect supported automation actions to DIAL-powered validation before execution. The underlying application and adapter determine the operation and its platform support.

### Vendor and OS coverage

Device interaction spans Cisco IOS/IOS XE, NX-OS and API-managed environments, Juniper Junos, Arista EOS, HPE Aruba, Palo Alto PAN-OS, Fortinet FortiOS, F5 TMOS, and other vendor platforms. Coverage varies by application and operation.

> **Working with the wider platform**
>
> Device Manager, OS Manager, and Config Model Editor use the platform's device-interaction capabilities. Titan's Intelligent MCP Server uses DIAL-powered validation to check proposed AI actions before execution.

**Supports:** Shared foundation across the capability stack.