# Activate Firmware Update Mode, Technique T0800 - ICS

Archived: 2026-04-05 15:40:01 UTC

| ID | Mitigation | Description |
|---|---|---|
| M0801 | Access Management | All devices or systems changes, including all administrative functions, should require authentication. Consider using access management technologies to enforce authorization on all management interface access attempts, especially when the device does not inherently provide strong authentication and authorization functions. |
| M0800 | Authorization Enforcement | Restrict configurations changes and firmware updating abilities to only authorized individuals. |
| M0802 | Communication Authenticity | Protocols used for device management should authenticate all network messages to prevent unauthorized system changes. |
| M0937 | Filter Network Traffic | Filter for protocols and payloads associated with firmware activation or updating activity. |
| M0804 | Human User Authentication | Devices that allow remote management of firmware should require authentication before allowing any changes. The authentication mechanisms should also support Account Use Policies, Password Policies, and User Account Management |
| M0807 | Network Allowlists | Use host-based allowlists to prevent devices from accepting connections from unauthorized systems. For example, allowlists can be used to ensure devices can only connect with master stations or known management/engineering workstations. [2] |
| M0930 | Network Segmentation | Segment operational network and systems to restrict access to critical system functions to predetermined management systems. [2] |

| ID | Mitigation | Description |
| --- | --- | --- |
| M0813 | Software Process and Device Authentication | Authenticate connections fromsoftware and devices to prevent unauthorized systems from accessing protected management functions. |

---

Source: https://attack.mitre.org/techniques/T0800