# / MAURISEC.DE

FIELD NOTES / CHECKLIST 06

# Intune: Endpunktschutz wirksam ausrollen

PRUEFEN. BELEGEN. NACHHALTEN.

Für von Intune unterstützte und entsprechend lizenzierte Geräte. Plattform und Betriebssystemedition je Prüfschritt berücksichtigen; BitLocker und ASR hier beziehen sich auf unterstützte Windows-Szenarien. Quellenstand: 09.11.2026.

Pruefbereich / Team:

Datum:

- [ ] **01 / Verwaltete Plattformen, unterstützte Versionen, Gerätezuständigkeiten und benötigte Sicherheitsfunktionen erfassen.**

  Nachweis: Datierter Gerätebestand mit Supportstatus und dokumentierten Ausnahmen.

- [ ] **02 / Je Einstellung festlegen, ob Baseline, Endpoint-Security- oder Konfigurationsprofil zuständig ist.**

  Nachweis: Richtlinienmatrix ohne widersprüchliche Mehrfachkonfiguration; geprüfte Konfliktberichte.

- [ ] **03 / Sicherheitskonfiguration zuerst in einer repräsentativen Pilotgruppe mit Rücknahmeweg ausrollen.**

  Nachweis: Pilotzuweisung, Funktionstests, Fehlerauswertung und Freigabe.

- [ ] **04 / Antivirus-, Firewall- und sonstige vorgesehene Schutzfunktionen am Gerät und im Verwaltungsbericht prüfen.**

  Nachweis: Aktueller Gerätestatus und erfolgreiche Richtlinienanwendung statt nur vorhandener Profilzuweisung.

- [ ] **05 / Vor BitLocker-Aktivierung Wiederherstellung planen und den autorisierten Zugriff auf Recovery-Informationen testen.**

  Nachweis: Verschlüsselungsbericht und geschützter Recovery-Test; keine Wiederherstellungsschlüssel im Checklisten-PDF.

- [ ] **06 / ASR-Regeln risikogerecht pilotieren; Audit-Ergebnisse und notwendige Ausnahmen vor breiter Durchsetzung auswerten.**

  Nachweis: ASR-Bericht, legitime Anwendungstests und begründete, eng begrenzte Ausnahmen.

# / MAURISEC.DE

FIELD NOTES / CHECKLIST 06

- [ ] **07 / Compliance-Anforderungen, Gültigkeitszeitraum und Verhalten für Geräte ohne zugewiesene Compliance-Richtlinie prüfen.**

  Nachweis: Tenant-Einstellungen und Gerätestatus; beabsichtigte Behandlung nicht bewerteter Geräte nachgewiesen.

- [ ] **08 / Compliance-basierten Zugriff in Conditional Access erst mit Aufnahme-, Notfall- und Negativtests erzwingen.**

  Nachweis: Erfolgreiche Geräteaufnahme sowie erwartete erlaubte und blockierte Testanmeldungen.

- [ ] **09 / Fehler, Konflikte, ausbleibende Check-ins und neue Baseline-Versionen regelmäßig nachverfolgen.**

  Nachweis: Betriebsbericht mit zuständiger Person und terminiertem Maßnahmenplan.

## GEGENPROBE / AUTORISIERTE TESTUMGEBUNG

An einem freigegebenen Pilotgerät den Unterschied zwischen Richtlinienzuweisung und tatsächlich wirksamer Einstellung nachweisen.

## GRENZEN UND VORAUSSETZUNGEN

Compliance-Bewertung ersetzt keine Härtungskonfiguration. Richtlinienzuweisung beweist keine erfolgreiche Anwendung. Plattformen und Editionen unterstützen unterschiedliche Einstellungen. ASR-Audit blockiert nicht; Warn-Modus kann eine Benutzerumgehung erlauben. Vor Verschlüsselungs- oder Zugriffseinschränkungen Wiederherstellung und Geräteaufnahme sicherstellen. Ein regelkonformes Gerät ist dadurch nicht nachweislich kompromissfrei.

## PRIMAERQUELLEN / STAND 09.11.2026


**Microsoft Learn: Endpoint security in Intune**
learn.microsoft.com

**Microsoft Learn: Manage endpoint security policies**
learn.microsoft.com

**Microsoft Learn: Device compliance overview**
learn.microsoft.com

**Microsoft Learn: BitLocker encryption with Intune**
learn.microsoft.com

**Microsoft Learn: ASR rules overview**
learn.microsoft.com