Safe Deployment Practices
FortiClient EMS

Version 7.4

Date: May 2026

1. Executive Summary

Fortinet provides FortiClient endpoint security software and FortiClient Enterprise Management Server (EMS) to enterprise customers globally. This document describes the Safe Deployment Practices (SDP) that govern how FortiClient software is released, validated, deployed, monitored, and recovered.

FortiClient deployments are customer-managed through FortiClient EMS. Fortinet does not directly deploy software into customer environments. Instead, Fortinet provides deployment controls, release validation processes, monitoring capabilities, rollback mechanisms, and operational guidance that enable customers to implement safe deployment strategies within their own organizations.

This document demonstrates that FortiClient EMS provides enterprise-grade deployment controls that meet or exceed industry-standard SDP requirements, including:

- Staged and phased rollout capabilities
- Real-time deployment monitoring and telemetry
- Version rollback and recovery mechanisms
- Emergency hotfix deployment
- Release validation and quality assurance processes
- Incident response and escalation procedures

2. Product Overview

2.1 FortiClient EMS

FortiClient Enterprise Management Server (EMS) is a centralized management platform that enables IT administrators to deploy, configure, monitor, and manage FortiClient instances across the organization. EMS provides the operational controls that enable Safe Deployment Practices in customer environments.

Key EMS deployment capabilities include:

- Endpoint group management and targeting
- FortiClient version deployment and upgrade management
- Version rollback and reversion controls
- Deployment scheduling and phased rollout
- Deployment status monitoring and health dashboards
- Telemetry collection, event logging, and compliance reporting
- Feature enablement and configuration profile management
- Emergency hotfix deployment

3. Deployment Architecture and Responsibility Model

The following model describes the end-to-end deployment lifecycle from Fortinet release to customer production deployment.

Deployment Lifecycle
1. Fortinet Internal Development & Code Review
2. Automated Testing (unit, integration, regression)
3. Quality Assurance Validation
4. Security Validation & Penetration Testing
5. Release Candidate Build & Signing
6. General Availability Release (Fortinet Portal)
7. Customer Downloads Signed Package
8. FortiClient EMS — Pilot Group Deployment
9. Deployment Monitoring & Health Validation
10. Staged Expansion to Broader Groups
11. Full Production Deployment
12. Rollback (if deployment issues detected)

Fortinet is responsible for steps 1 through 7. Customer IT administrators using FortiClient EMS are responsible for steps 8 through 12. This model allows customers to retain full operational control over endpoint deployment decisions while Fortinet ensures software quality, security, and availability.

4. Internal Release Validation and Quality Assurance

Prior to any public release, FortiClient software passes through a formal release validation pipeline.

4.1 Development and Code Review

All code changes undergo peer review before integration. Security-sensitive changes receive additional review from the security engineering team.

4.2 Automated Testing

An automated test suite covering unit tests, integration tests, and regression tests is executed against every build. Test failures block promotion to the next stage.

4.3 Quality Assurance Validation

QA teams perform functional testing, platform compatibility testing across supported Windows OS versions, and validation against the supported platform matrix published in release notes.

4.4 Security Validation

Security validation includes static analysis, vulnerability scanning, and security acceptance criteria checks. Critical and high severity findings are resolved before release.

4.5 Release Candidate and Signing

A release candidate build is produced and signed using Fortinet's code signing certificate. Signed packages ensure authenticity and integrity of distributed software.

4.6 Release Documentation

Each release is accompanied by:

- Official release notes documenting changes, resolved issues, and known limitations
- Supported OS and platform matrix
- Upgrade and downgrade guidance
- Security advisory notices where applicable

Reference: https://docs.fortinet.com/document/forticlient/7.4.7/ems-release-notes/717049/introduction

5. Staged Rollout Capabilities

FortiClient EMS provides administrators with the controls needed to implement staged and phased deployment strategies.

5.1 Endpoint Groups

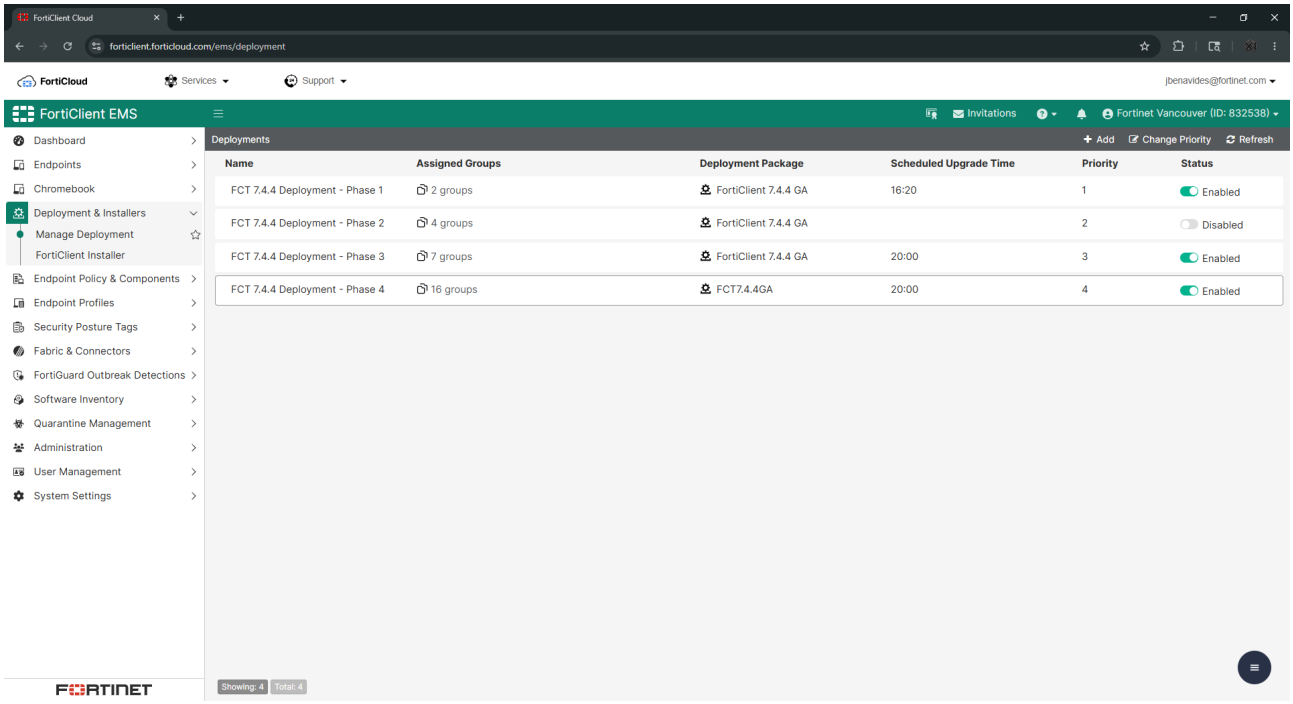
Administrators define endpoint groups to segment the population by role, department, geography, or risk level. Deployment actions can be targeted at specific groups, enabling ring-based deployment strategies.

5.2 Pilot Deployment

A pilot group — typically a subset of technical or volunteer users — receives the new FortiClient version first. Deployment health is monitored before expanding rollout scope.

5.3 Phased Expansion

After pilot validation, deployment is expanded to progressively larger groups. EMS deployment packages allow administrators to define which version is deployed to each group independently.



5.4 Deployment Scheduling

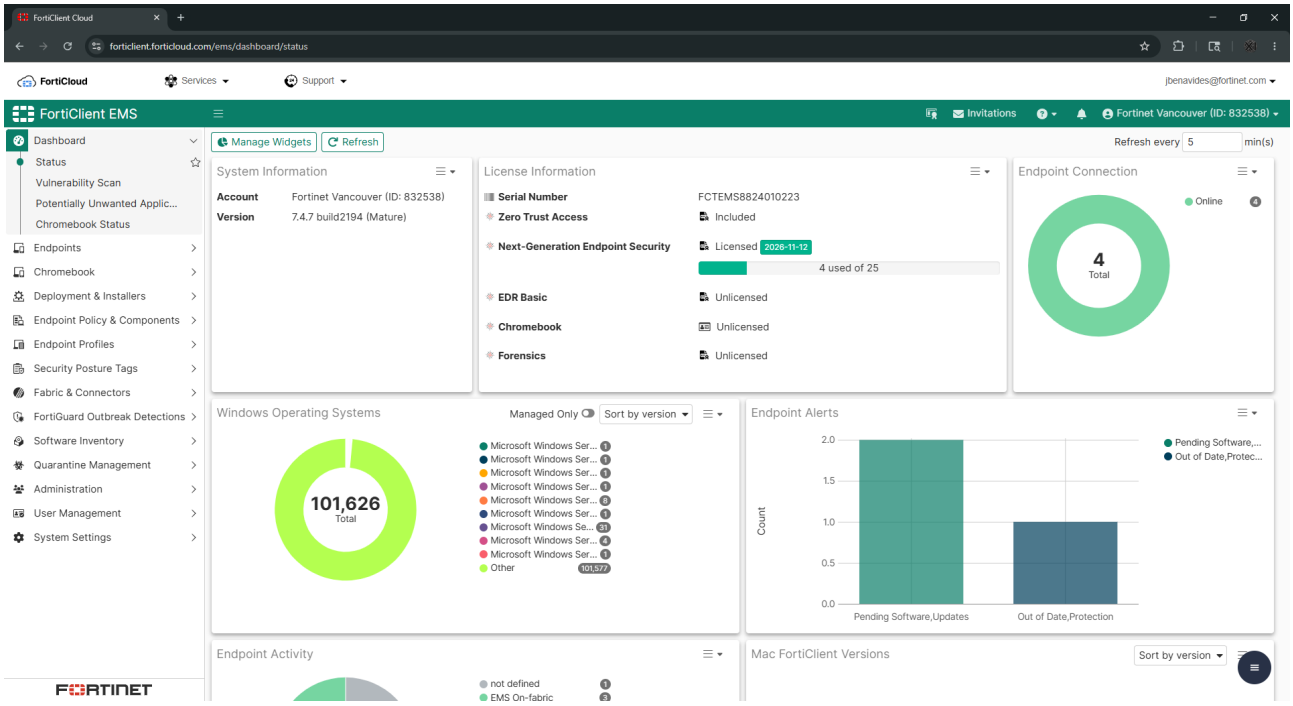
EMS supports scheduled deployments, allowing rollouts to be staged across maintenance windows or time zones to minimize operational impact.

6. Deployment Monitoring and Observability

FortiClient EMS provides centralized visibility into deployment health and endpoint status.

6.1 Deployment Status Dashboard

The EMS dashboard provides real-time visibility into endpoint deployment status, including the number of endpoints on each FortiClient version, registration status, and connectivity status.

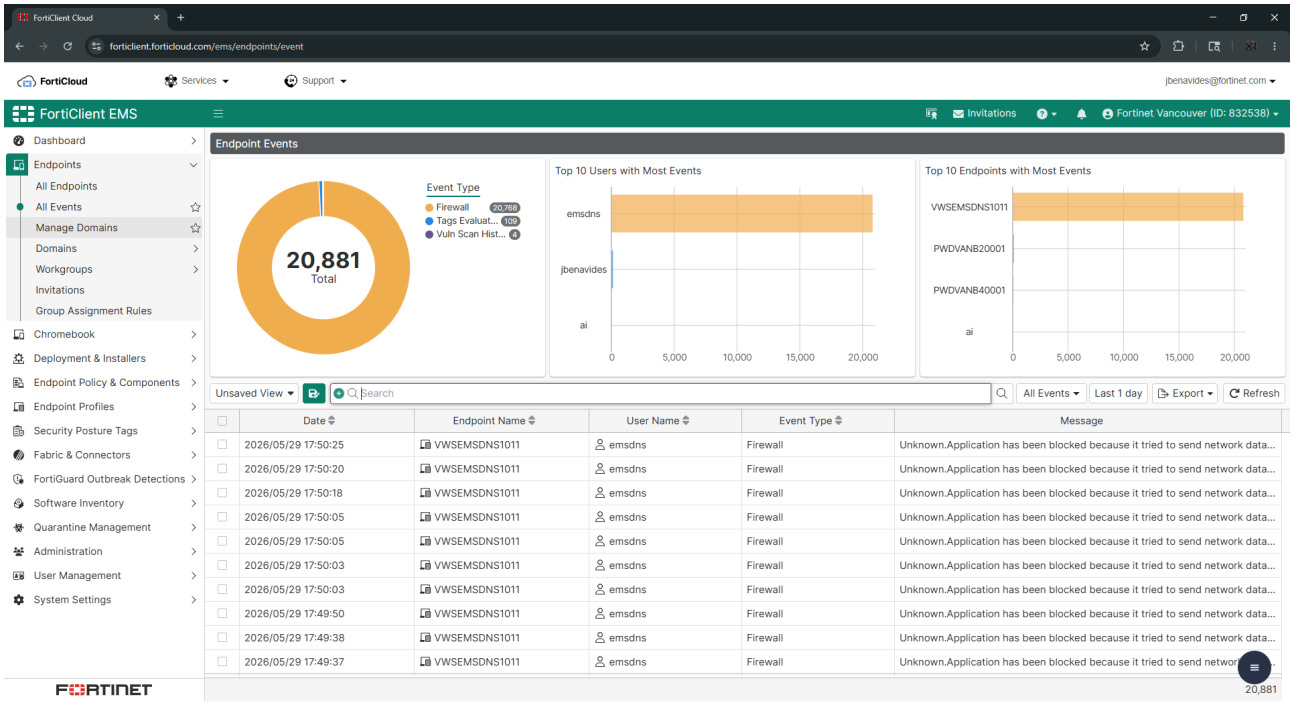


6.2 Endpoint Health Monitoring

EMS monitors endpoint health, including client running status, VPN connectivity, ZTNA posture, and security profile compliance.

6.3 Telemetry and Event Collection

FortiClient endpoints report telemetry events to EMS including client version, policy compliance status, vulnerability scan results, and security events. This data enables administrators to assess deployment quality across the endpoint population.



7. Rollback and Recovery Capabilities

FortiClient EMS provides mechanisms to revert endpoints to previously approved software versions in the event of a deployment issue.

7.1 Version Rollback

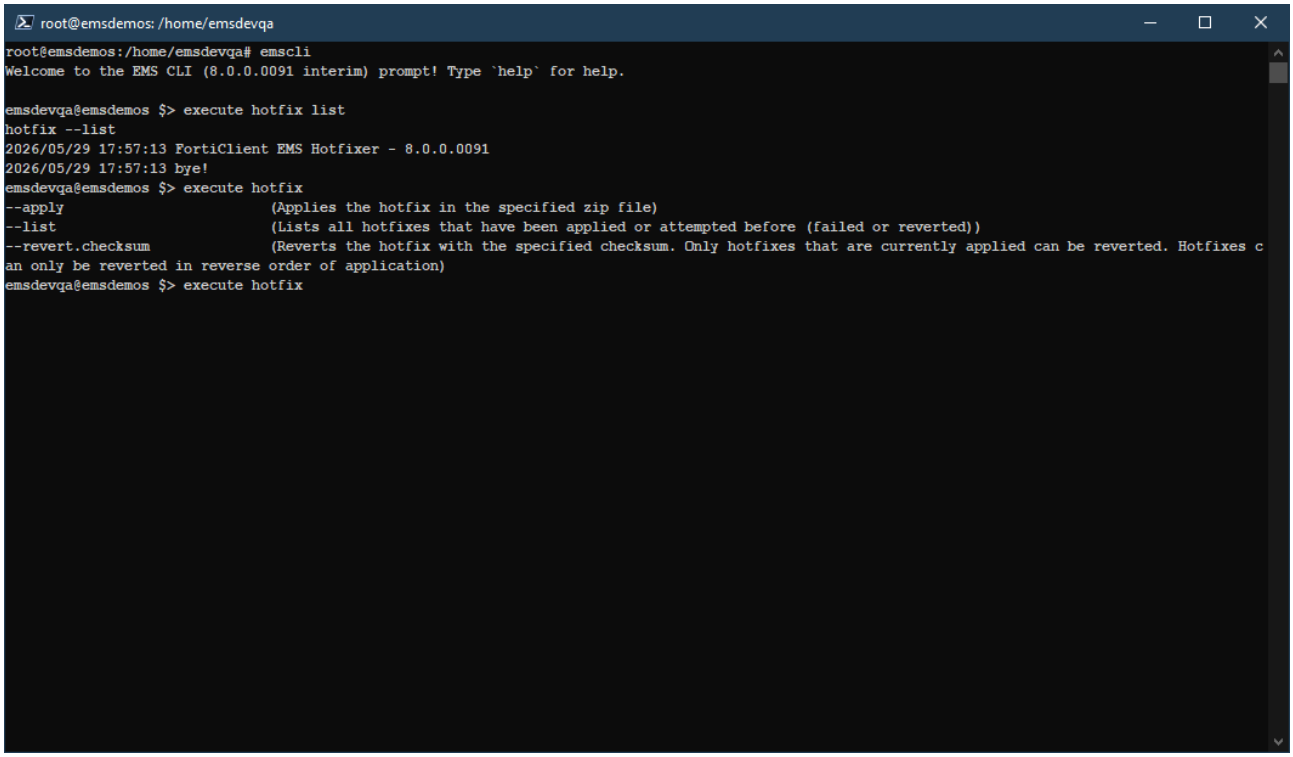
Administrators can create a deployment package targeting a previously approved FortiClient version and deploy it to affected endpoint groups. EMS supports deploying any previously downloaded and validated build.

7.2 Targeted Rollback

Rollback can be targeted to specific endpoint groups or individual endpoints, enabling surgical remediation without affecting the broader endpoint population.

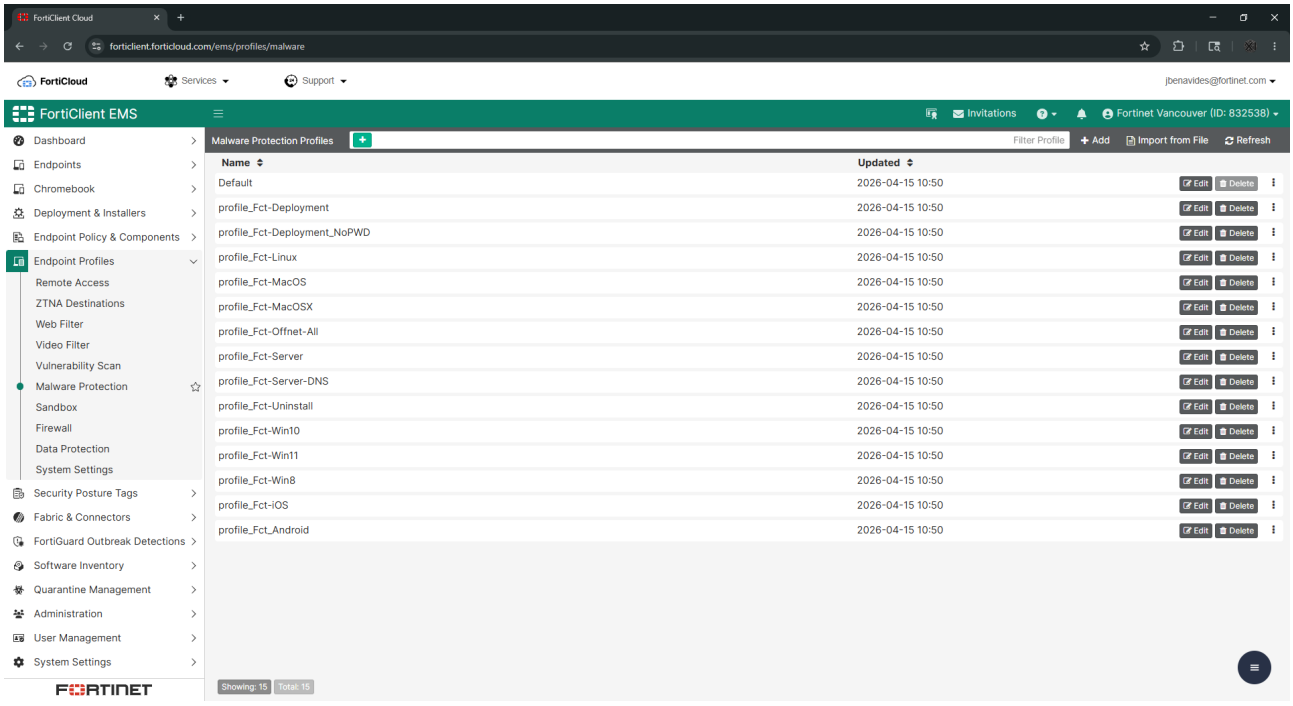
7.3 Emergency Hotfix Deployment

In urgent cases, Fortinet may issue an emergency hotfix release. EMS administrators can deploy hotfix packages immediately to all or selected endpoints without waiting for a scheduled maintenance window.



7.4 Configuration Rollback

Independent of software version, EMS administrators can revert configuration profiles applied to endpoints. This allows configuration issues to be fixed without full software redeployment.



8. Incident Response and Emergency Procedures

8.1 Deployment Issue Response

If deployment-related issues are detected, the recommended response procedure is:

- Halt ongoing deployment activities for affected groups
- Assess deployment telemetry and event logs in EMS to identify scope and root cause
- Limit rollout scope or quarantine affected groups in EMS
- Revert affected endpoints to the last approved stable version using EMS rollback
- Engage Fortinet Technical Assistance Center (TAC) if root cause is unclear or a software defect is suspected
- Deploy corrective hotfix or configuration update once validated
- Document incident, root cause, and resolution for post-incident review

8.2 Fortinet TAC Escalation

Customers may escalate deployment issues to Fortinet TAC at any time. TAC provides:

- Root cause analysis support
- Rollback guidance
- Hotfix coordination if a software defect is identified
- Emergency release support for critical vulnerabilities

8.3 Security Vulnerability Response

If any security vulnerability is identified in a released FortiClient version, Fortinet follows its Product Security Incident Response Team (PSIRT) process:

- Vulnerability assessment and severity classification
- Development and validation of a security fix
- Security advisory publication via the Fortinet PSIRT portal
- Notification to affected customers
- Emergency release or hotfix deployment through EMS

9. SDP Evidence Summary

The following table summarizes the SDP areas covered in this submission and the evidence provided or referenced.

SDP Area	Typical Evidence
Staged Rollout	Screenshots: deployment rings, pilot groups, phased deployment settings in EMS
Monitoring	Screenshots: deployment status dashboard, telemetry, endpoint health reports
Rollback	Screenshots: version selection, reversion workflow, emergency update targeting

Emergency Response	Runbook: escalation steps, hotfix deployment procedure, stakeholder notification
Release Validation	QA workflow: automated testing gates, regression results, release qualification checklist
Version Management	Screenshots: upgrade controls, version pinning, deployment targeting
Deployment Approval	Admin approval workflow, deployment authorization controls
Observability	Logging, alerting, compliance reporting, event telemetry examples

10. References and Documentation

Official Fortinet documentation is available through the Fortinet Documentation Portal:

- FortiClient Documentation Portal: https://docs.fortinet.com/product/forticlient/7.4
- FortiClient EMS Administration Guide: https://docs.fortinet.com/document/forticlient/7.4.7/ems-administration-guide/24450/introduction
- Fortinet PSIRT: https://www.fortiguard.com/psirt