# CN213: Mirantis Secure Registry (MSR) (On Demand)

**Code:** CN213-OD
**URL:** View Online

In this product-focused course, you'll deep dive into all the features of Mirantis Secure Registry, and discover how it can enhance the security of your container image production, storage and distribution both as a stand-alone registry, or integrated into a continuous integration pipeline. We'll discuss installing and configuring MSR, managing MSR user permissions, enhancing registry security with content trust and binary security scanning, as well as registry management strategies like garbage collection, content caching, and webhook-driven third-party integrations.

**Benefit from vendor-certified IT training and get access to video content of certified instructor(s), one year of access to the course videos, and up to 240 hours of hands-on cloud-based labs over any 10 day period.**

# Who Can Benefit

This course is targeted at students with the following:

- Motivations: Leverage all the features of Mirantis Secure Registry in order to enhance the security profile of container image content, distribution and execution.
- Roles: System Operators & Administrators

# Prerequisites

- CN212 course and prerequisites therein, or equivalent experience
- Familiarity with the Bash shell
- Filesystem navigation and manipulation
- Command line text editors like vim or nano
- Common tooling like curl, wget and ping
- Familiarity with YAML and JSON notation

## Course Details

### Lab Requirements

- Laptop with WiFi connectivity
- Attendees should have the latest Chrome or Firefox installed, and a free account at strigo.io .

## Course Outline

Mirantis Secure Registry architecture

- Production-grade deployment patterns
- Containerized components of MSR
- Networking & System requirements for MSR
- Installing MSR via Launchpad for high availability
- Integrating external storage into MSR

Access control in MSR

- MSR RBAC system

Content Trust

- Defeating man in the middle attacks with The Update Framework & Notary
- Content Trust usage in MSR

Security Scanning

- Auditing container images for known vulnerabilities
- Setting up MSR security scanning
- Security scan integration in continuous integration

Repository Automation

- Continuous integration pipeline architecture featuring MSR
- Promoting and mirroring images through pipelines
- Integrating MSR with external tooling via webhooks

Image Management

- Image pruning and garbage collection strategies and automation
- Registry sizing strategy
- Content caching for distributed teams

MSR Troubleshooting

- Correlating MSR symptoms with components
- Probing and reading MSR state databases
- Recovering failed MSR replicas
- MSR backups & restore
- Disaster recovery in event of critical MSR failure

---