ABB IAPG Technology – Cyber Security

Security Workplace Package Overview and Maintain Demonstration

Power and productivity for a better world™

Security Workplace
Package Overview and Maintain Demonstration

- Speaker name: Joseph Catanese
- Speaker title: Manager, Cyber Security IAPG
- Company name: ABB Inc.
- Location: Wickliffe, Ohio
- Phone: 440-585-2789
- E-Mail: joseph.p.catanese@us.abb.com

Security Workplace
Presentation Outline

- Package Overview
- Maintain Package
- Defend Package
- Comply Package
- Continued Development
- Maintain Demonstration

Security Workplace

Package Overview

Security Workplace Package overview

Security Workplace

MAINTAIN
- **Centralized Microsoft Patching***
- Centralized Antivirus Management
- Centralized, Automated Backup and Recovery

COMPLY
- Security Event Monitoring
- Configuration Change Management
- ICS Asset Management
- Automated Compliance Reporting
- Policy Management
- Workflow Automation Suite

DEFEND OPTIONS
- **File Sanitizer (ODI-X)***
- Intelligent Whitelisting
- Network Segmentation and DMZ Implementation

* Indicates product is in managed release

Security Workplace
Package overview

Security Baseline Requirements**	MAINTAIN	COMPLY	DEFEND
Automated back-up & recovery	✓	✓	
Centralized anti-virus management	✓	✓	
Centralized Microsoft patch management	✓	✓	
Monitoring, Reporting and NERC CIP Compliance			
Security event management*		✓	
Configuration change management*		✓	
ICS asset management*		✓	
Automated compliance reporting*		✓	
Automated data collection*		✓	
Policy management*		✓	
Workflow Automation Suite		✓	
Active Defense Options			
Electronic perimeter protection			O
Intelligent application whitelisting			O
Security architecture, DMZ			O

*Available for Fleet-Wide and Multi-Vendor Control Systems

**Active ServiceGrid contract required

✓= Included

O = Optional Add-on to any package

Security Workplace

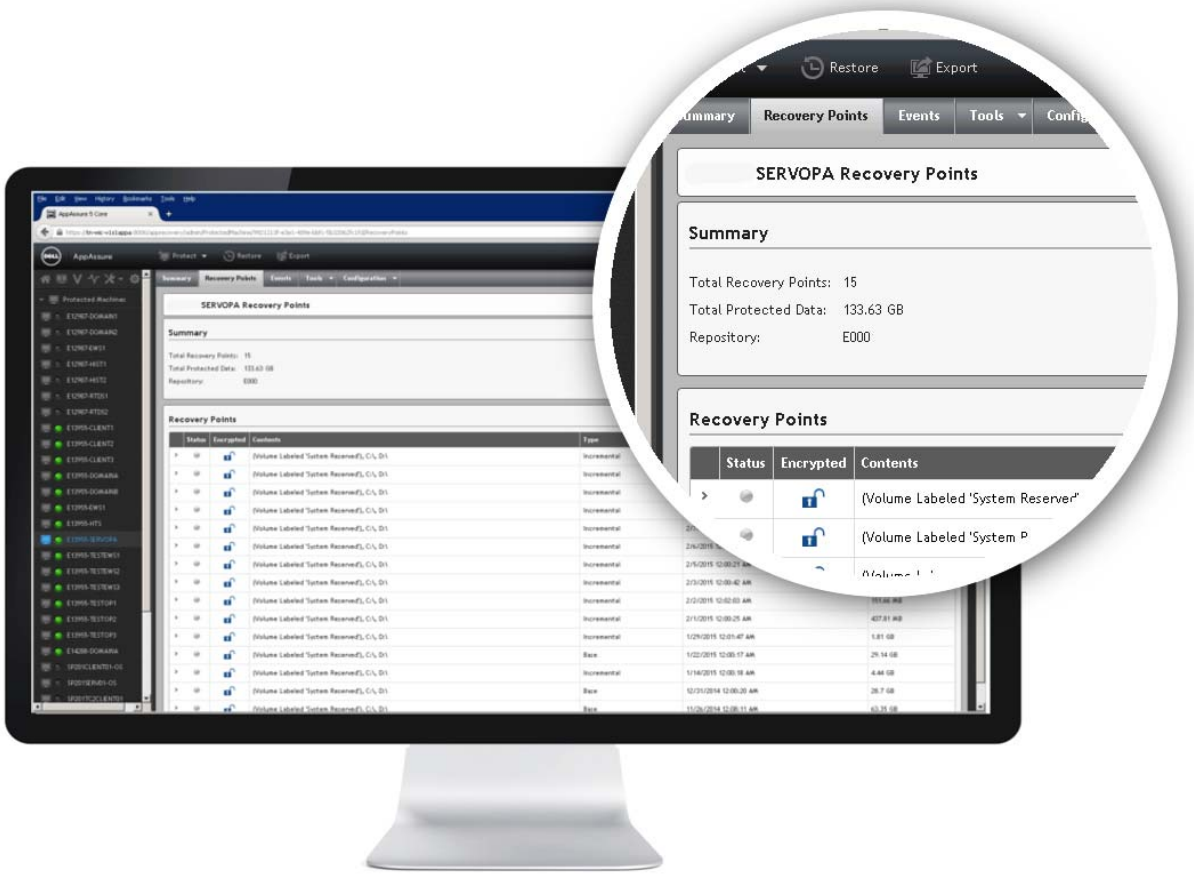
Maintain Package

ABB Security Workplace
Maintain

Automated Backup & Recovery

Centralized Anti-Virus Management

Centralized Microsoft Patch Management



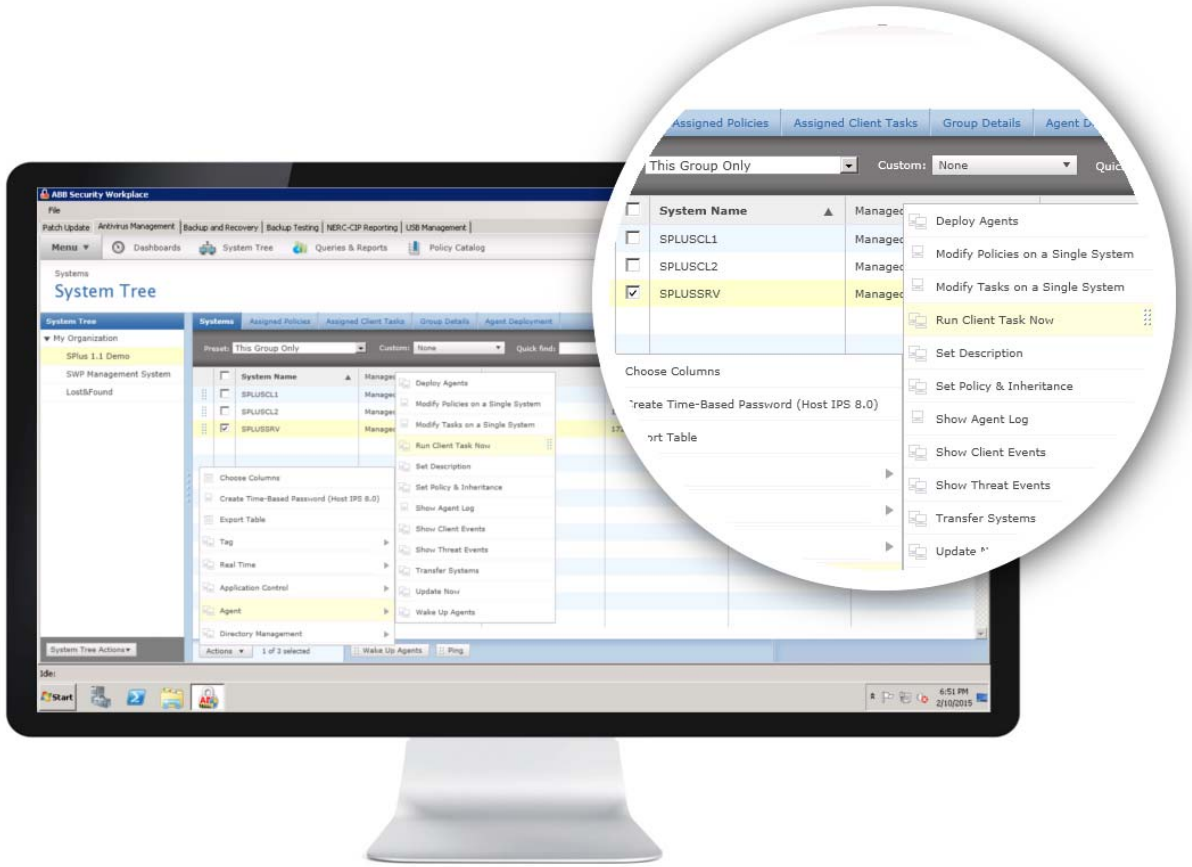
- Incremental-Daily-Weekly-Monthly
- Centrally manages backup plans
- Conversion to VM
- Deduplication/ Efficient backups

ABB Security Workplace
Maintain

Automated Backup & Recovery

Centralized Anti-Virus Management

Centralized Microsoft Patch Management



- Manage AV Policies
- Manage DAT file deployments

ABB Security Workplace
Maintain

Automated Backup & Recovery

Centralized Anti-Virus Management

Centralized Microsoft Patch Management

- IAPG developed and maintained
- Reduces effort in deploying Microsoft patching
- Aligned with ABB Validation Documents

Security Workplace

Comply Package

ABB Security Workplace
Comply

Security Event Management

Configuration Change Management

ICS Asset Management

Automated Compliance Reporting

Policy Management

Workflow Automation Suite

- Improve situational awareness
- Monitor system performance
- Consolidate event logs
- Detect anomalies
- Triage alerts
- Generate reports

ABB Security Workplace Comply

Security Event Management | **Configuration Change Management** | ICS Asset Management | Automated Compliance Reporting | Policy Management | Workflow Automation Suite

- Reduce manual activities by 80%
- Improve change management
- Eliminate configuration drift
- Report compliance effortlessly
- Improve control system cyber security

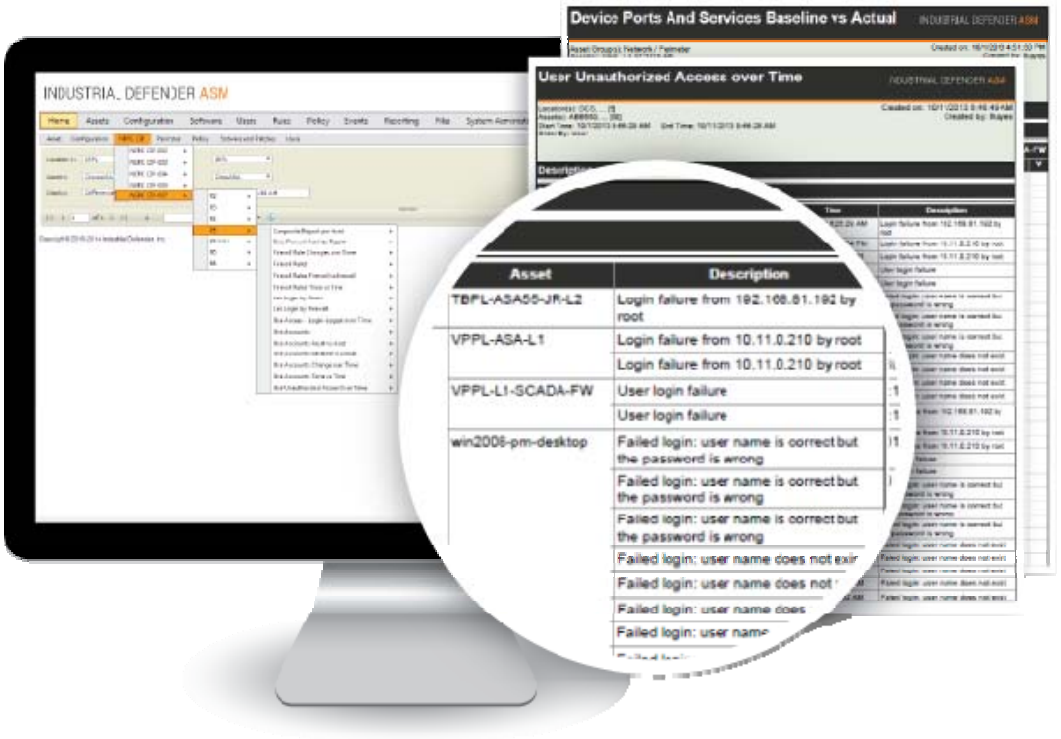
ABB Security Workplace Comply

Security Event Management | **Configuration Change Management** | **ICS Asset Management** | **Automated Compliance Reporting** | **Policy Management** | **Workflow Automation Suite**

- Reduce cyber security risks
- Meet compliance requirements
- Unified, single view of asset base

ABB Security Workplace Comply

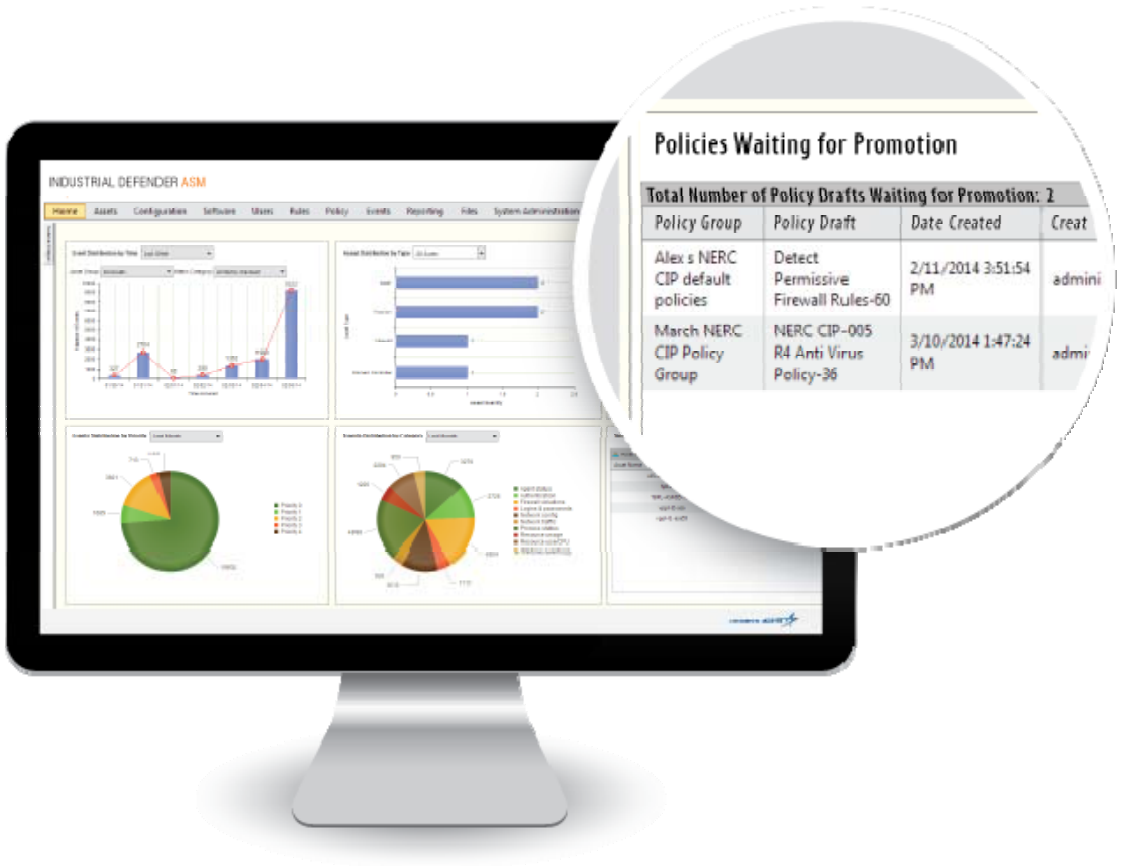
Security Event Management | **Configuration Change Management** | **ICS Asset Management** | **Automated Compliance Reporting** | **Policy Management** | **Workflow Automation Suite**



- NERC-CIP compliance
- Ports and services
- Software inventory
- Password policy
- User accounts

ABB Security Workplace
Comply

Security Event Management | **Configuration Change Management** | **ICS Asset Management** | **Automated Compliance Reporting** | **Policy Management** | **Workflow Automation Suite**



- Communicate new policies
- Track acceptance
- Manage conformance
- Always be audit-ready

ABB Security Workplace
Comply

Security Event Management | **Configuration Change Management** | **ICS Asset Management** | **Automated Compliance Reporting** | **Policy Management**

Workflow Automation Suite

- Initiate, track, approve, document and report on workflows
- Document management
- Automated reporting

Security Workplace

Defend Options

ABB Security Workplace
Defend Options

File Sanitization

Application Control

Network Segmentation/DMZ Implementation

- Control files entering your system
- Scan for viruses
- Prevents distributed attacks
- Easy and fast to use
- Files upload directly to share

ABB Security Workplace
Defend Options

File Sanitization

Application Control

Network Segmentation/DMZ Implementation

- Application whitelisting
- At-a-glance dashboard
- Easy policy creation
- Fully integrated into AV management console

ABB Security Workplace
Defend Options

File Sanitization

Application Control

Network Segmentation/DMZ Implementation

- Edge Routing/Firewall
- Unified Threat Manager
- IPSec / SSL VPN
- Transparent Firewall (FDI/Cnet)

Security Workplace

Continuing Development

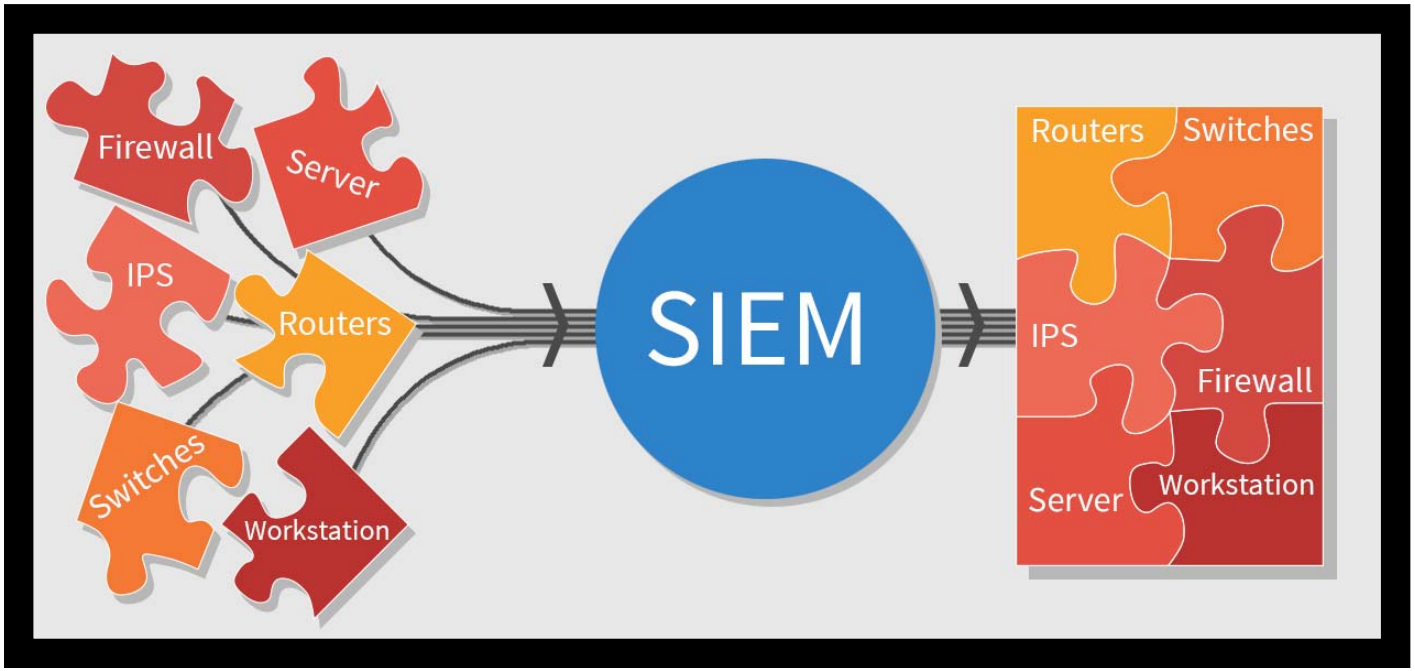
ABB Security Workplace
Continuing Development

Security Information and Event Monitoring (SIEM)

Device Control

Network Anomaly Detection

- Log aggregation
- Log correlation
- Intelligent alerting
- Customizable



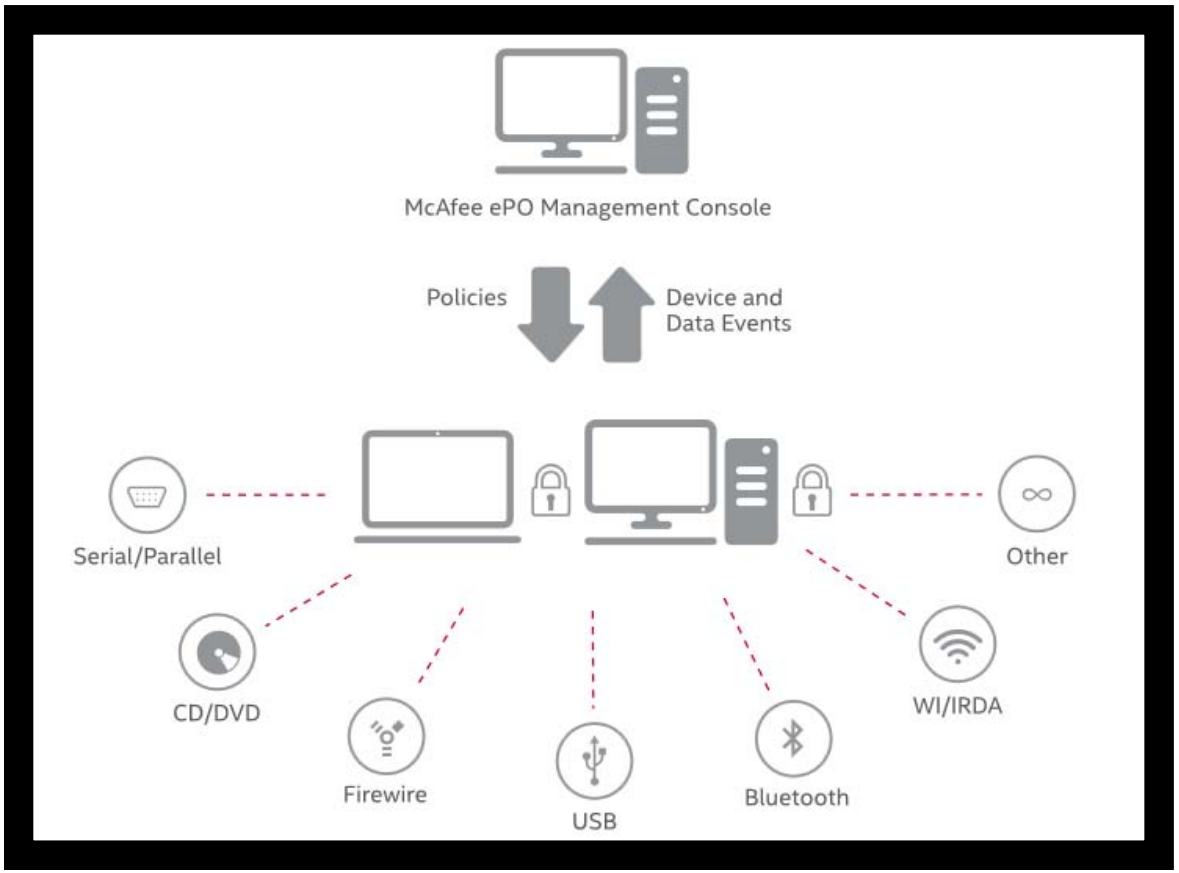
https://www.integritysrc.com/blog/122-benefits-of-log-consolidation-in-a-siem-environment

ABB Security Workplace
Continuing Development

Security Information and Event Monitoring (SIEM)

Device Control

Network Anomaly Detection



http://www.mcafee.com/us/resources/data-sheets/ds-device-control.pdf

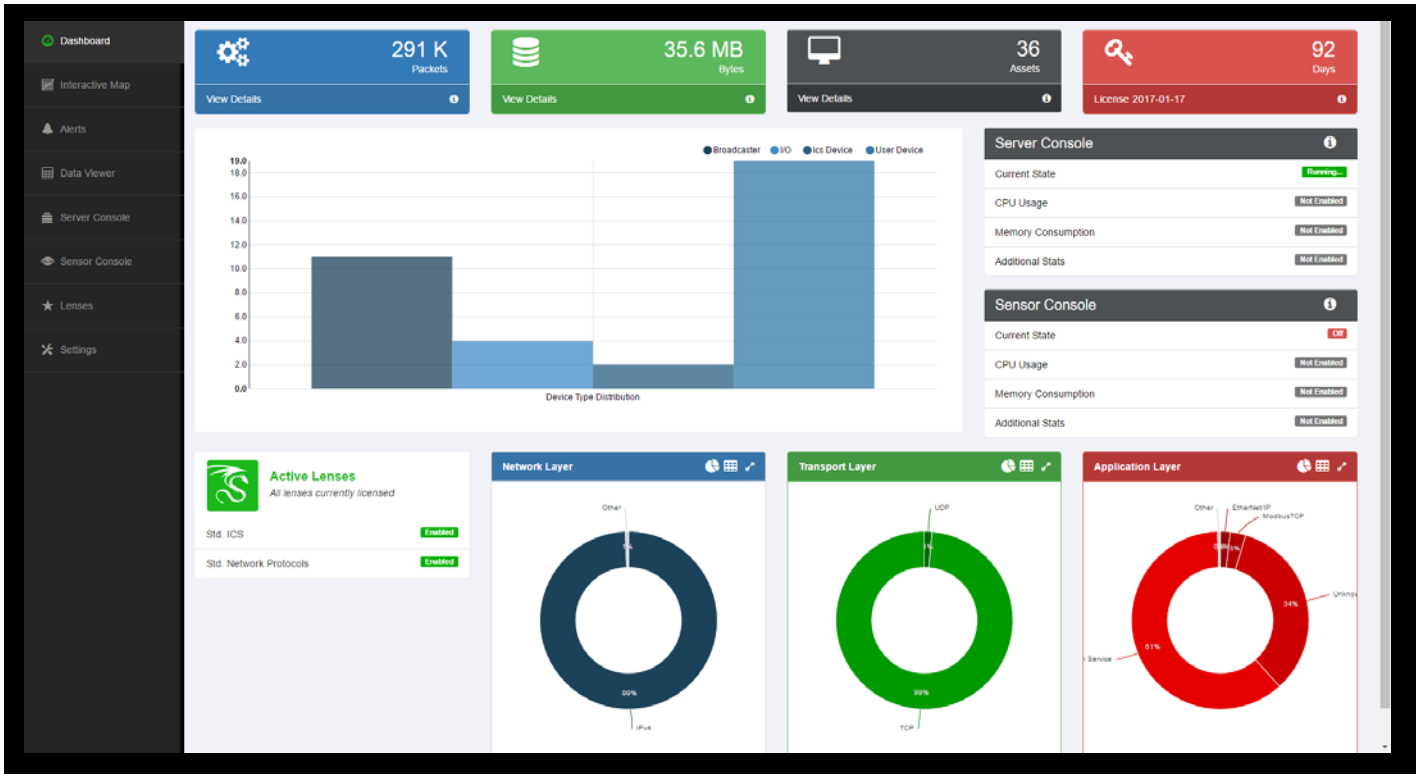
- Unrivaled data protection
- Comprehensive device management
- McAfee ePO centralized management platform
- Complete visibility

ABB Security Workplace
Continuing Development

Security Information and Event Monitoring (SIEM)

Device Control

Network Anomaly Detection



- Ongoing Evaluations
- Simple UI, Alerts
- Network Mapping
- DPI

Security Workplace

Maintain Package Demonstration

ABB Security Workplace
Maintain - Demonstration

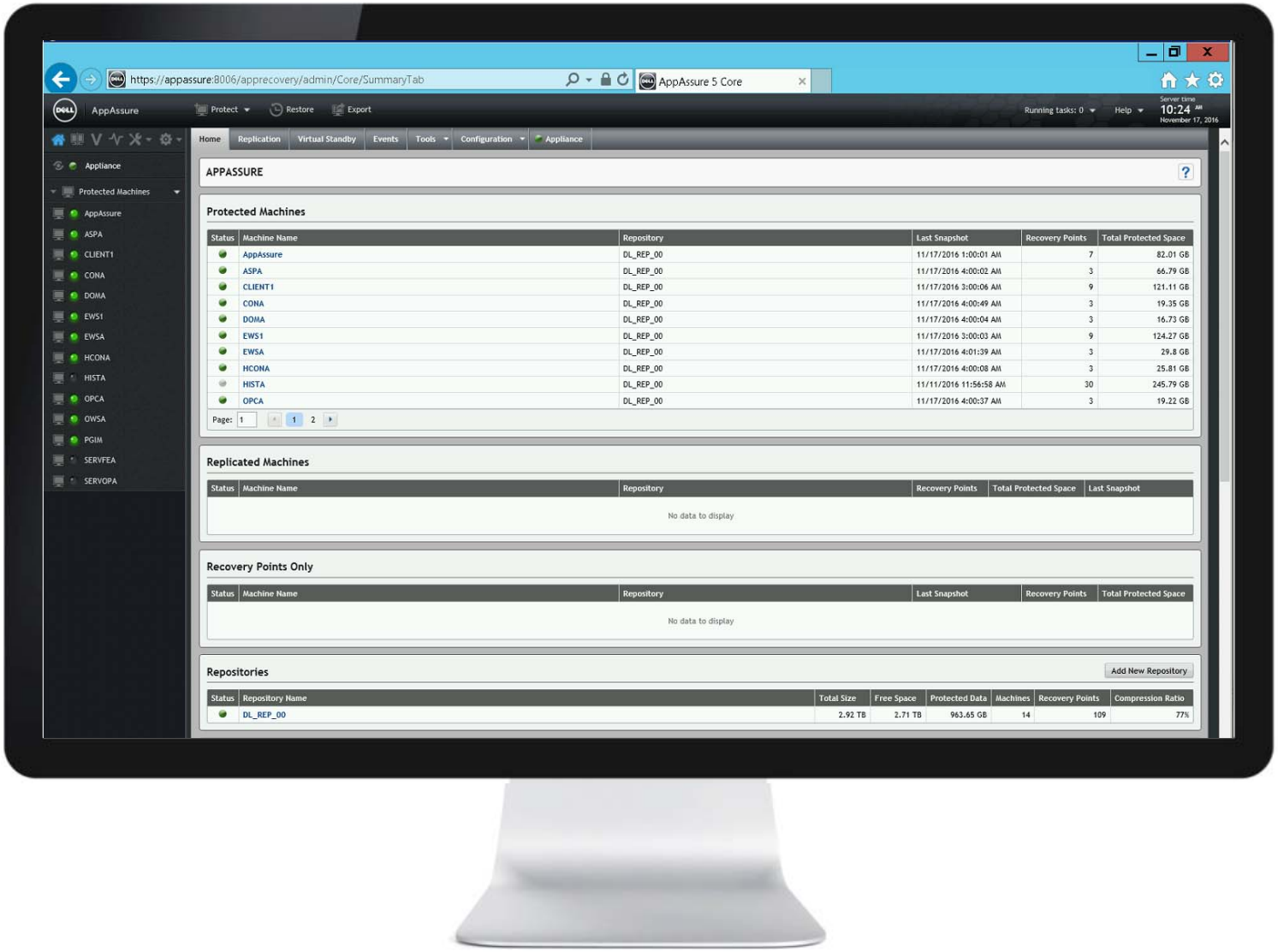


ABB Security Workplace
Maintain - Demonstration

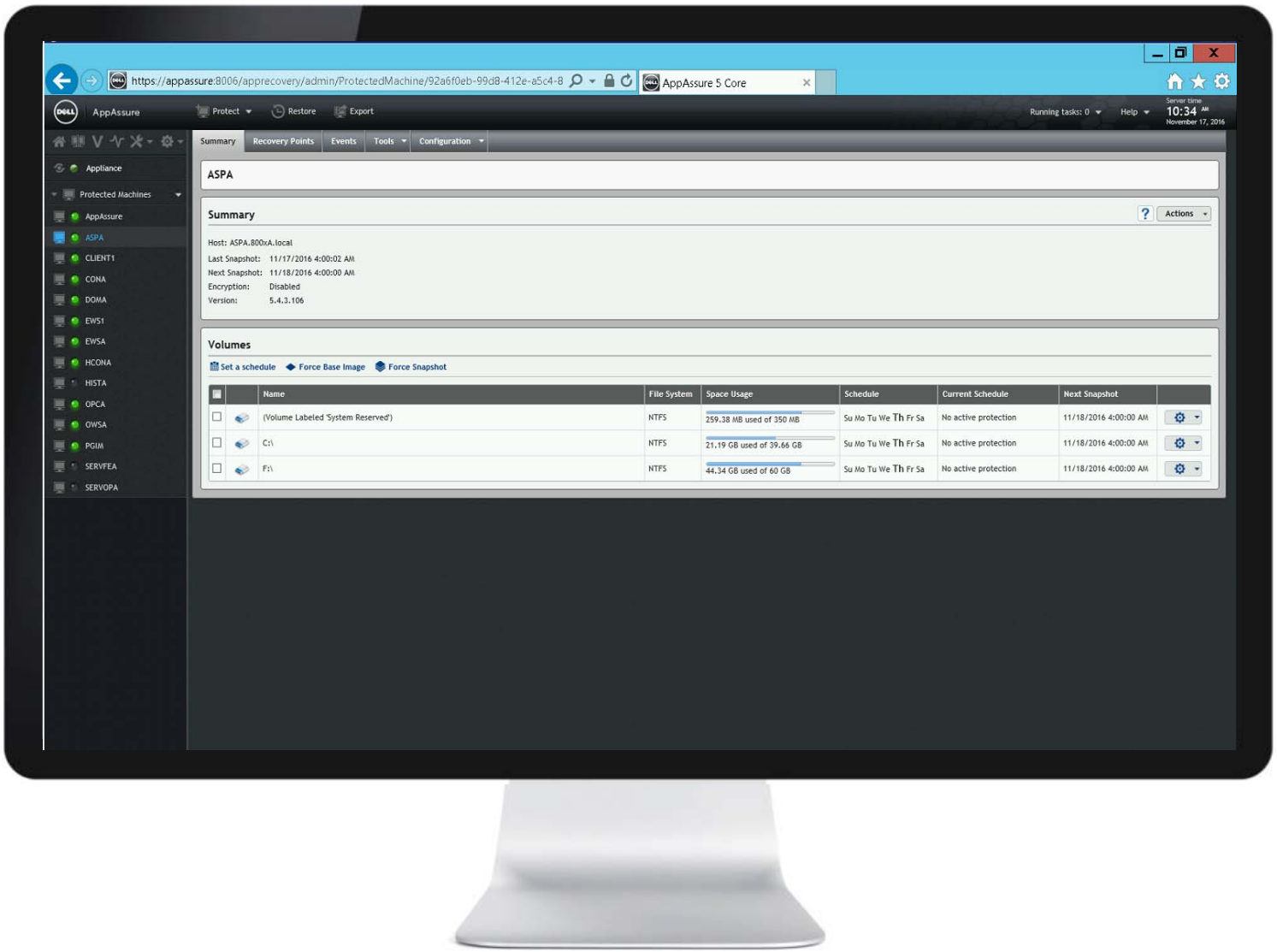


ABB Security Workplace
Maintain - Demonstration

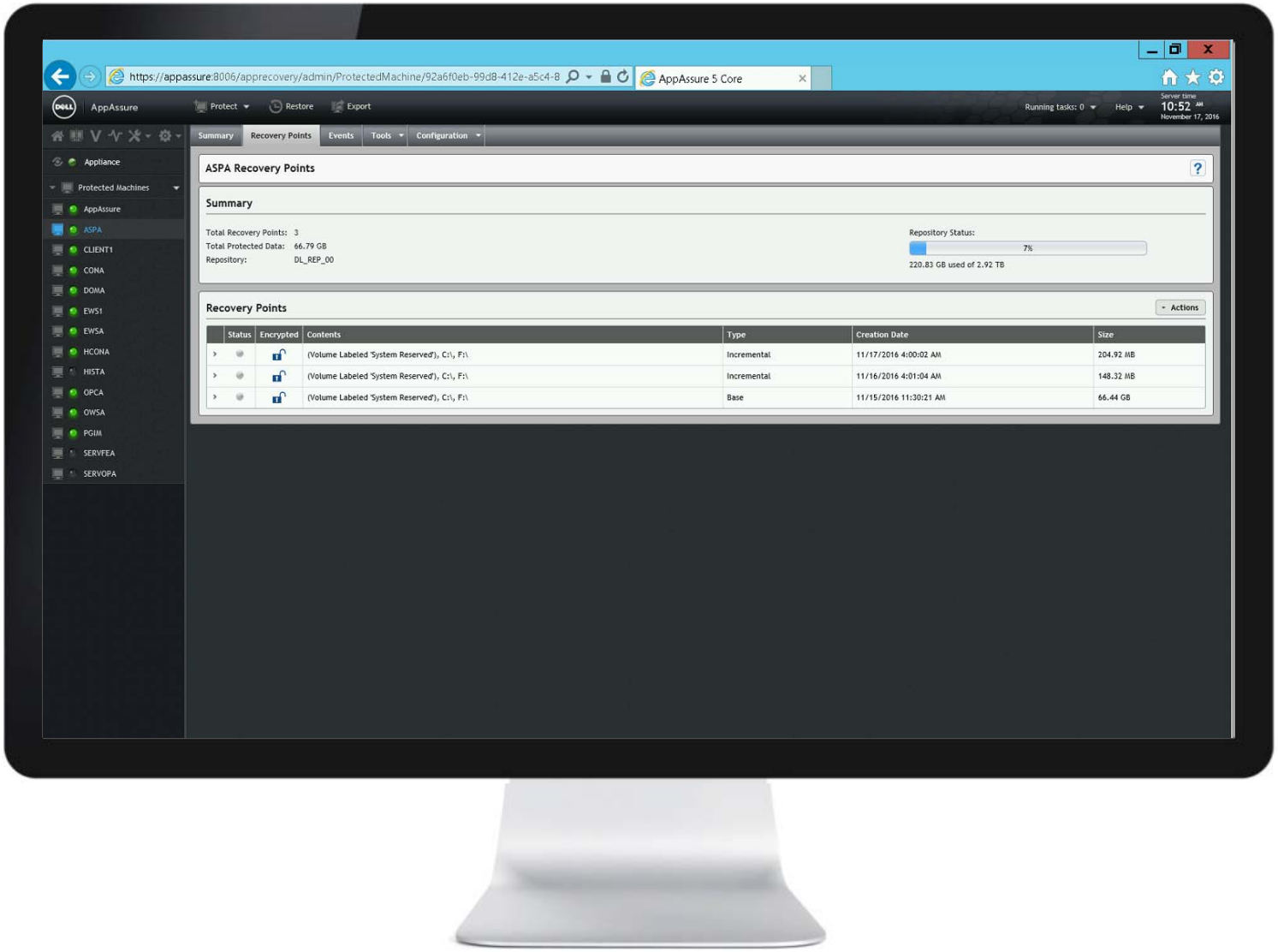


ABB Security Workplace
Maintain - Demonstration

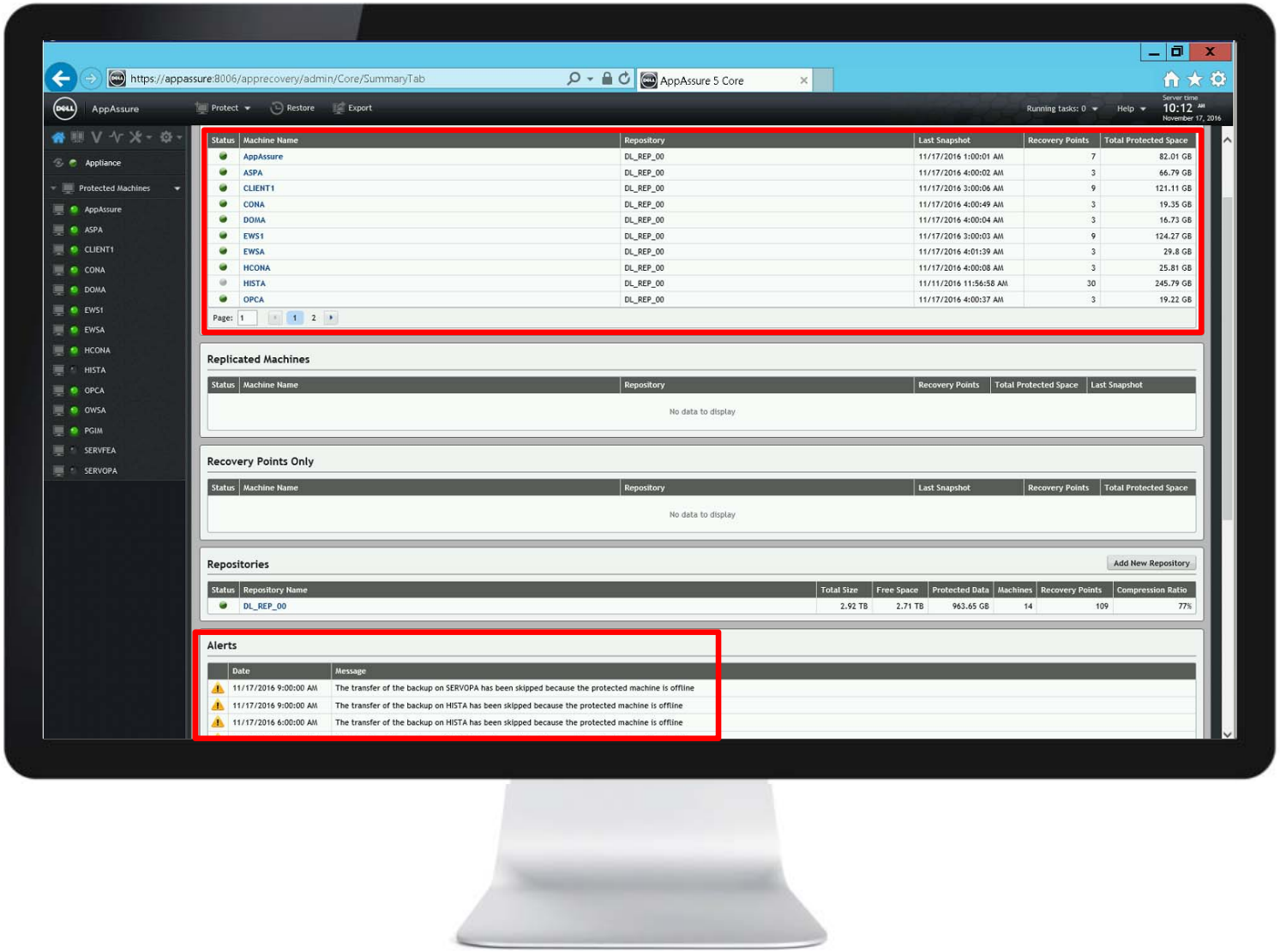


ABB Security Workplace
Maintain - Demonstration

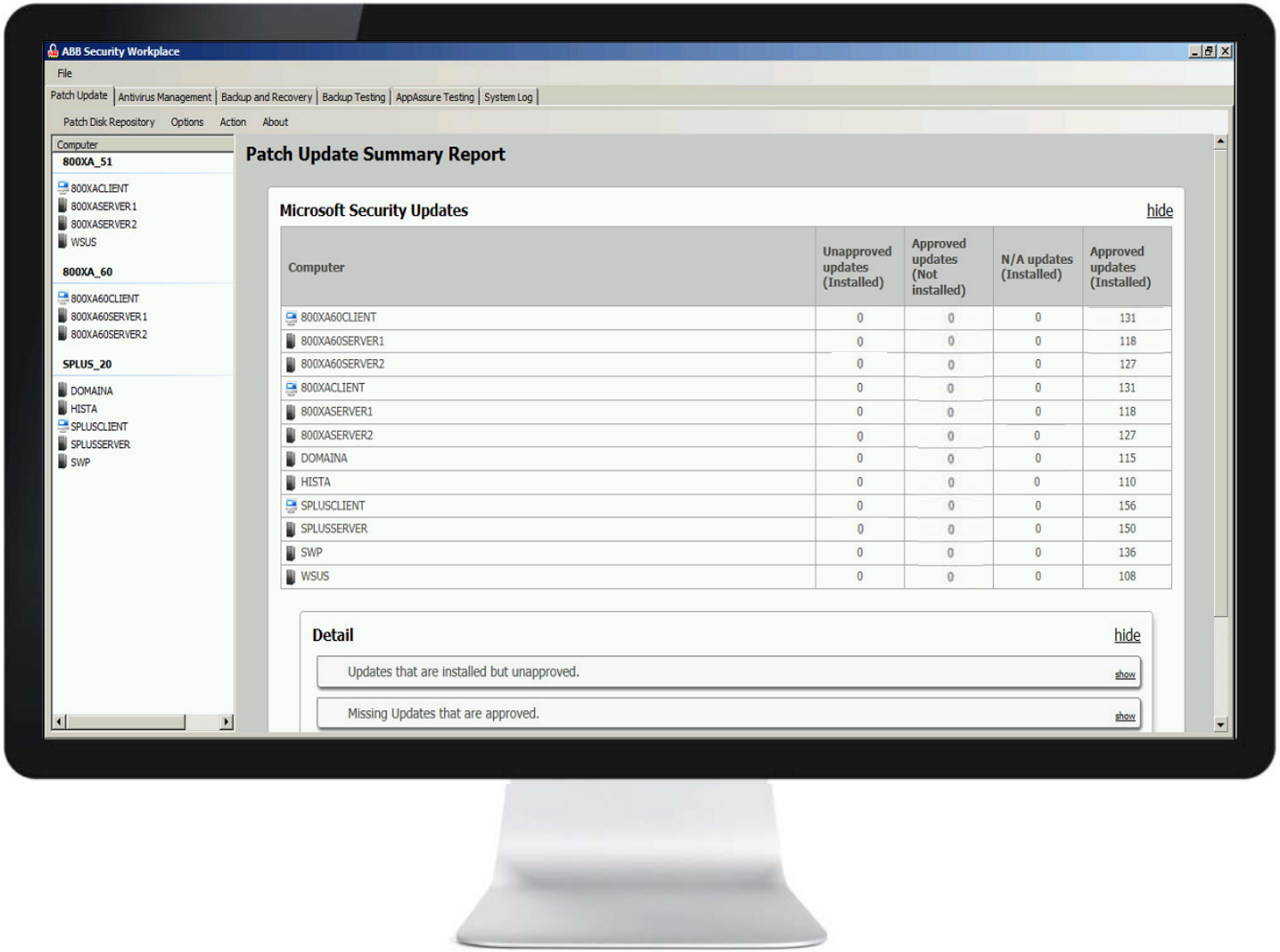


ABB Security Workplace
Maintain - Demonstration

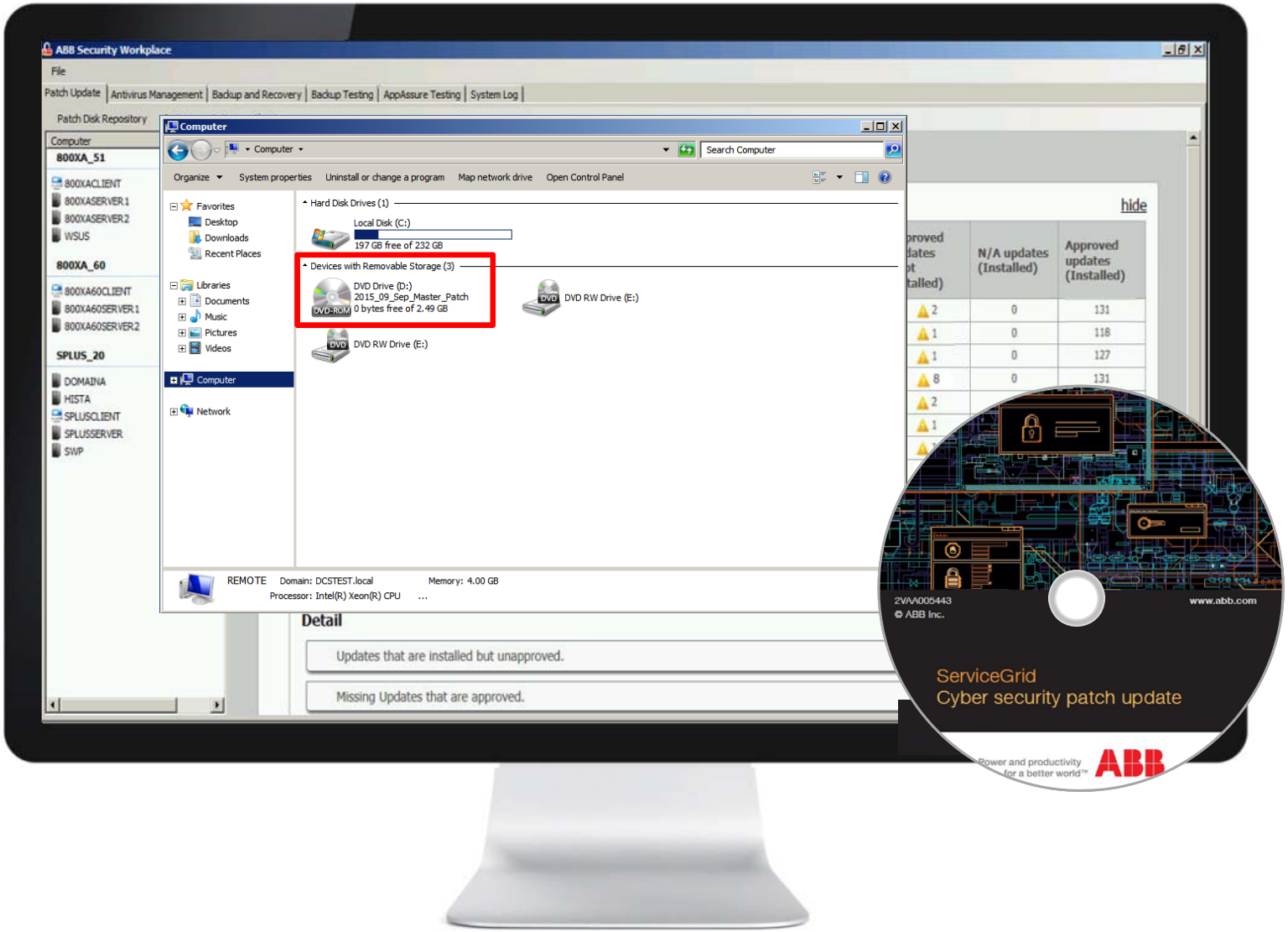


ABB Security Workplace
Maintain - Demonstration

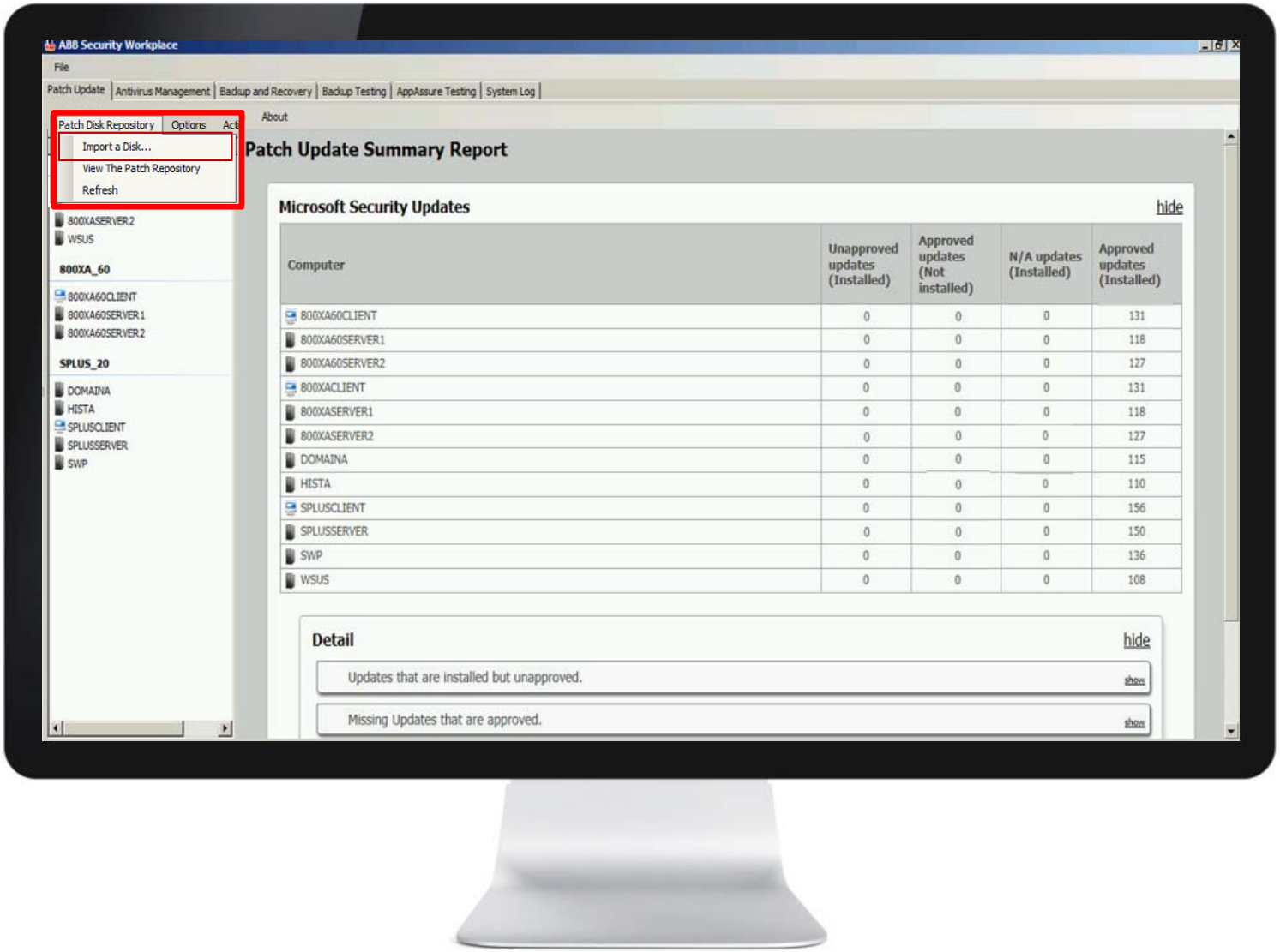


ABB Security Workplace
Maintain - Demonstration

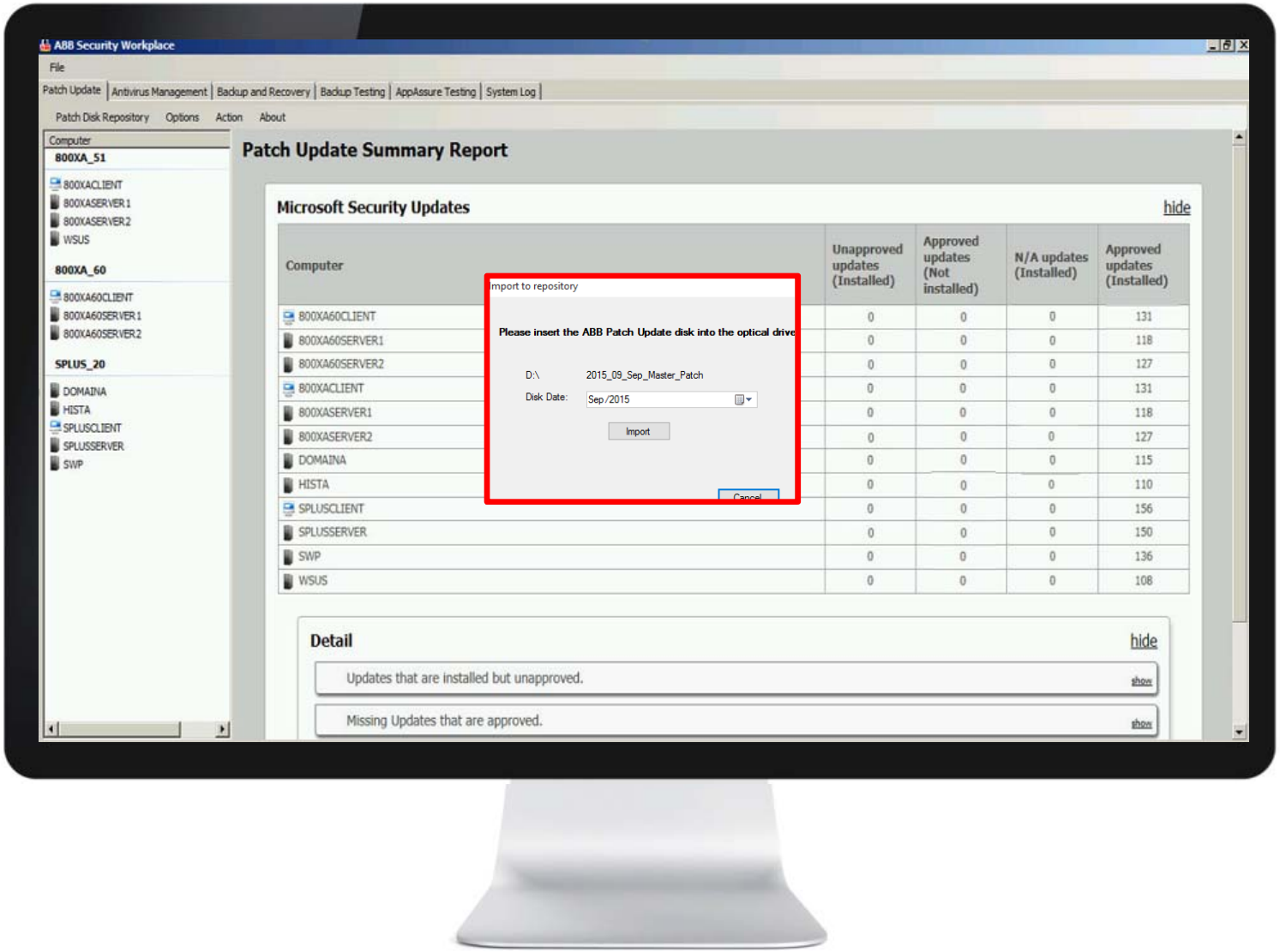


ABB Security Workplace
Maintain - Demonstration

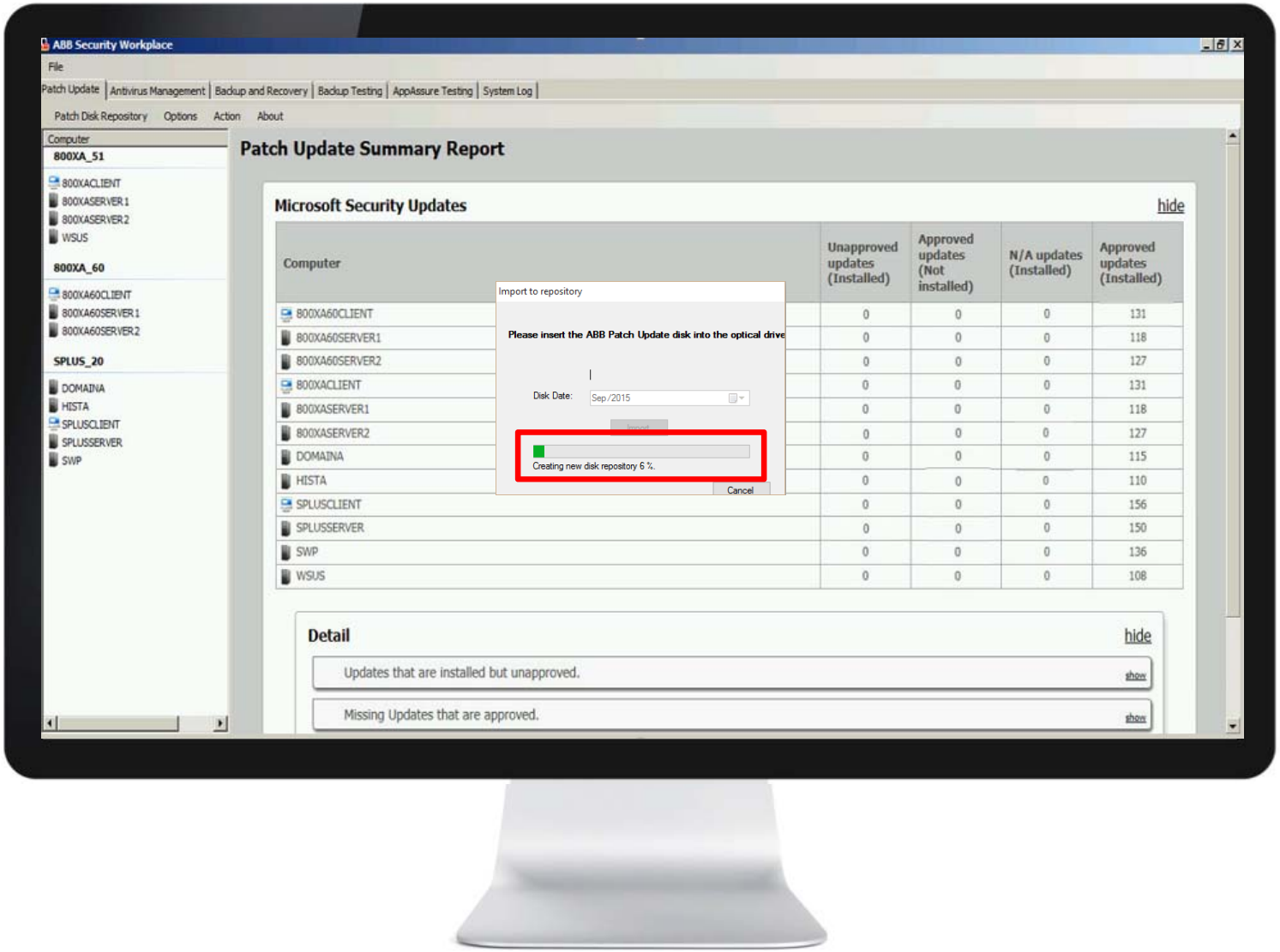


ABB Security Workplace
Maintain - Demonstration

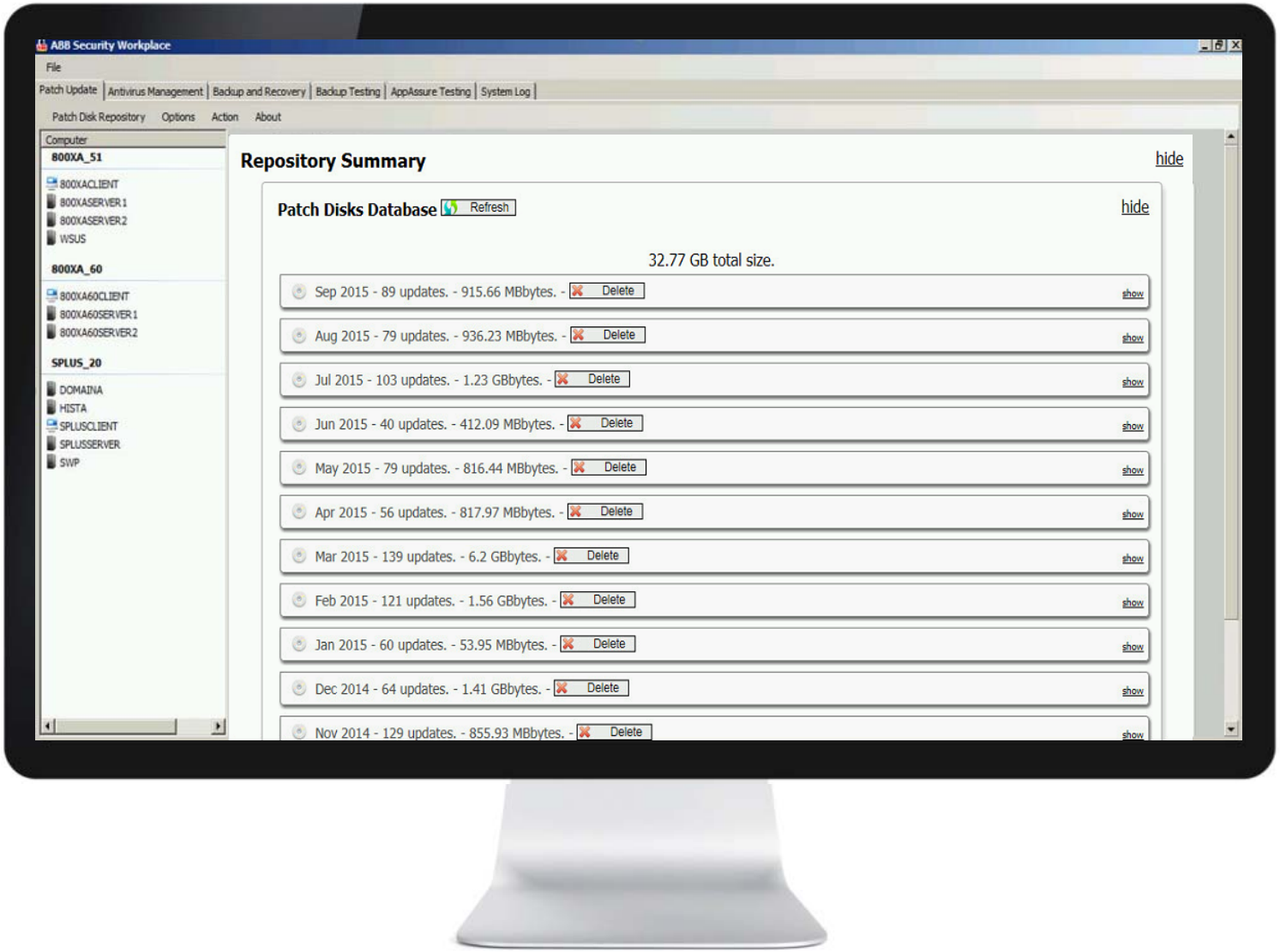


ABB Security Workplace
Maintain - Demonstration

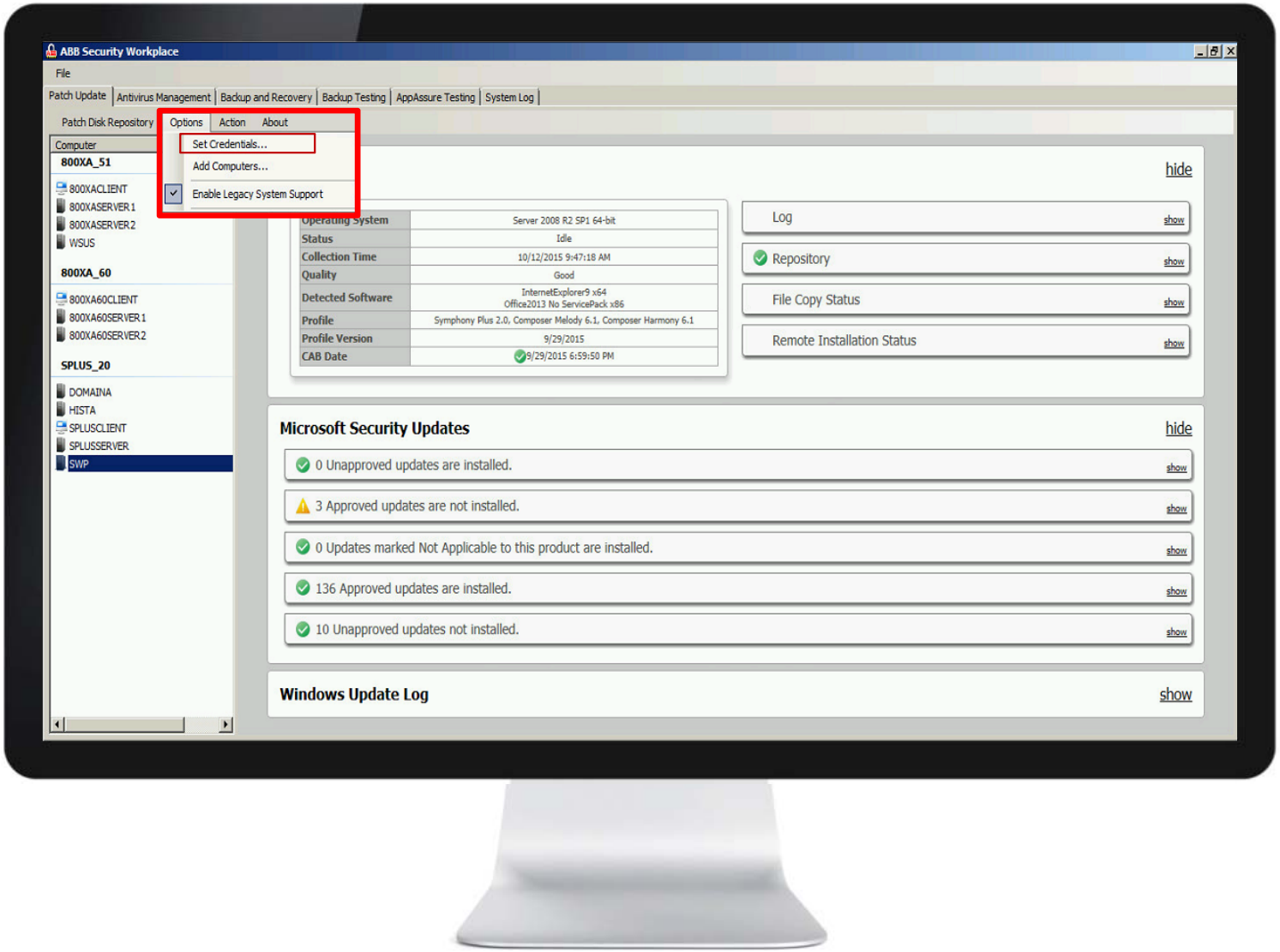


ABB Security Workplace
Maintain - Demonstration

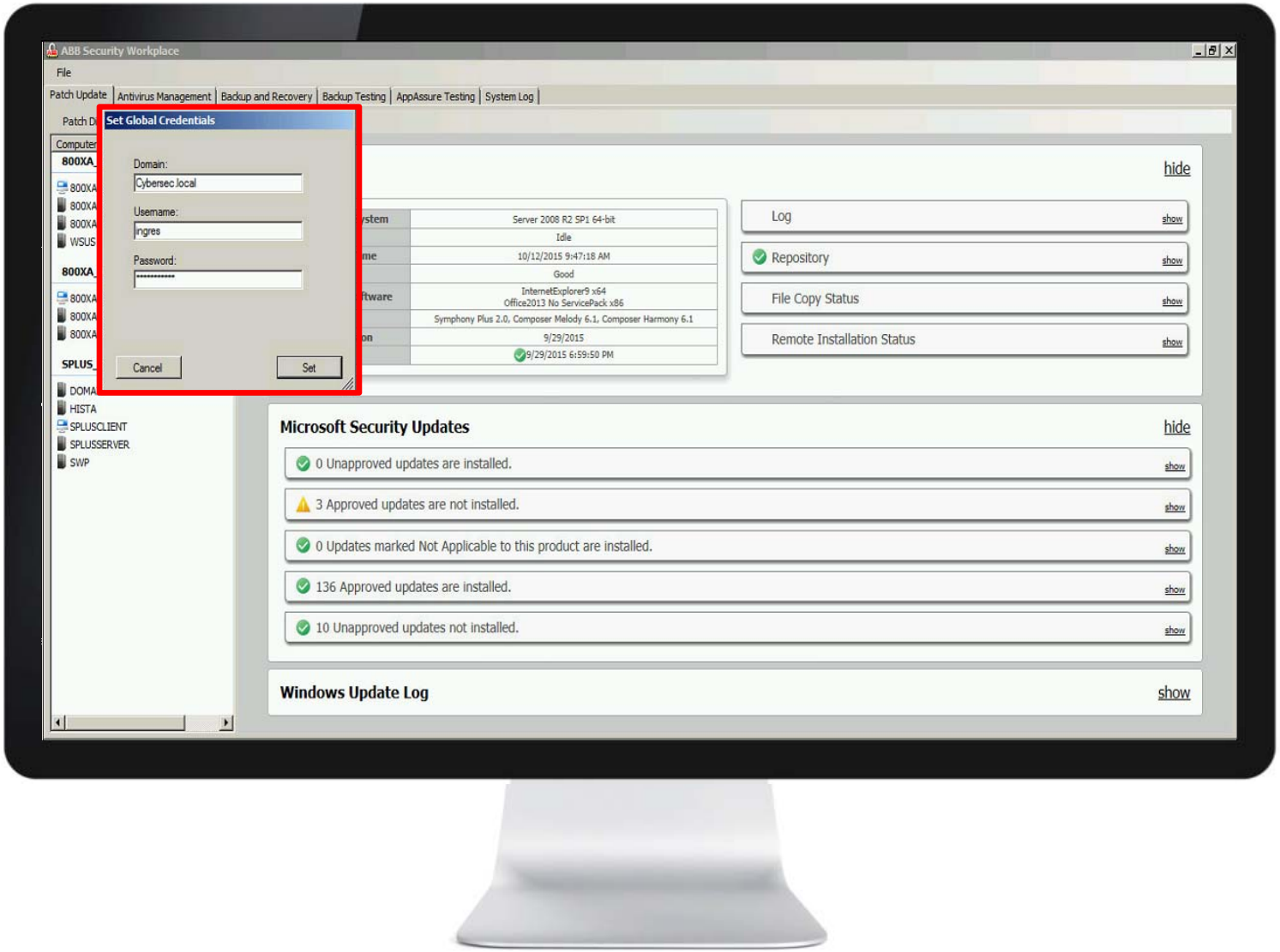


ABB Security Workplace
Maintain - Demonstration

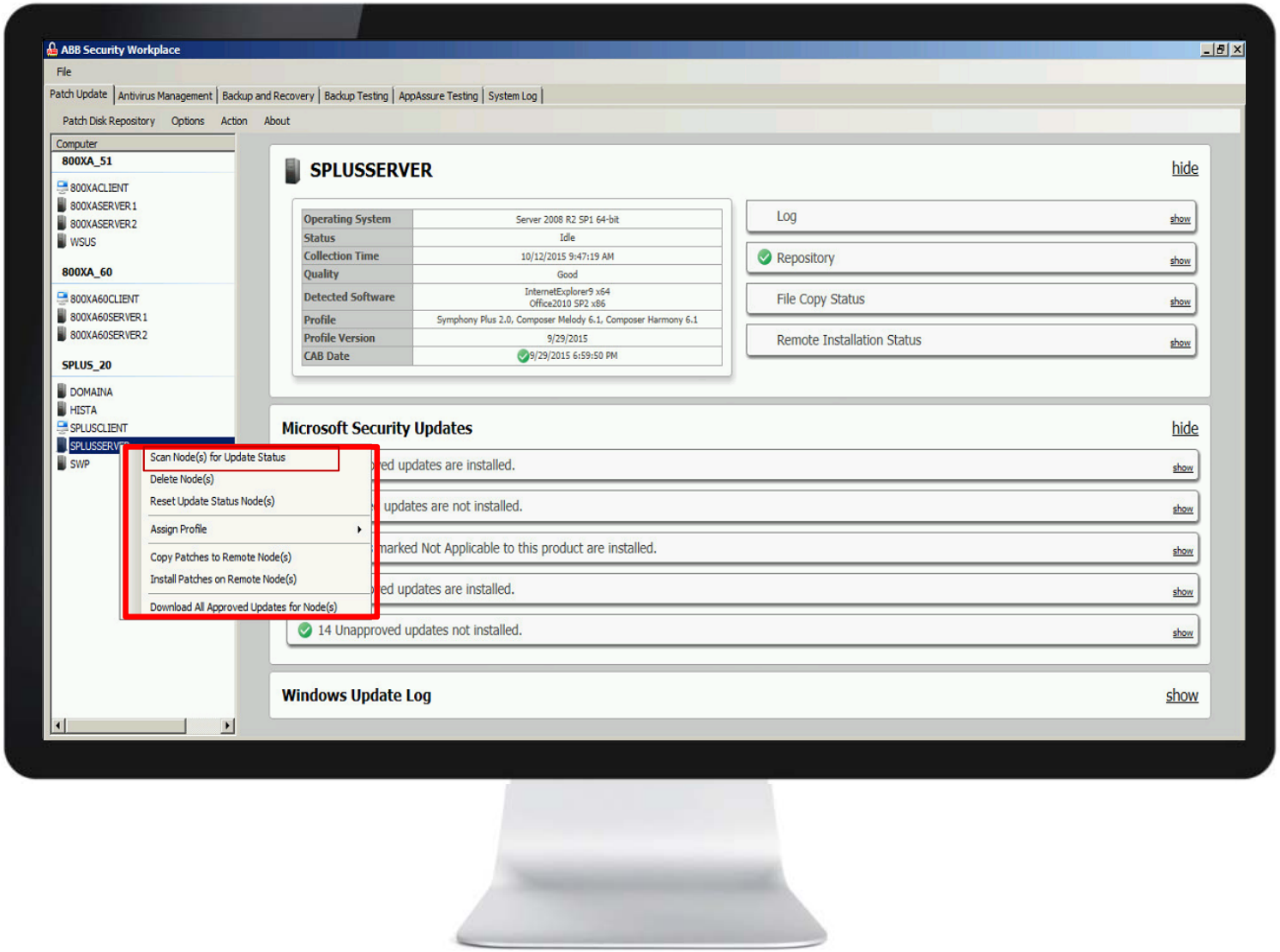


ABB Security Workplace
Maintain - Demonstration

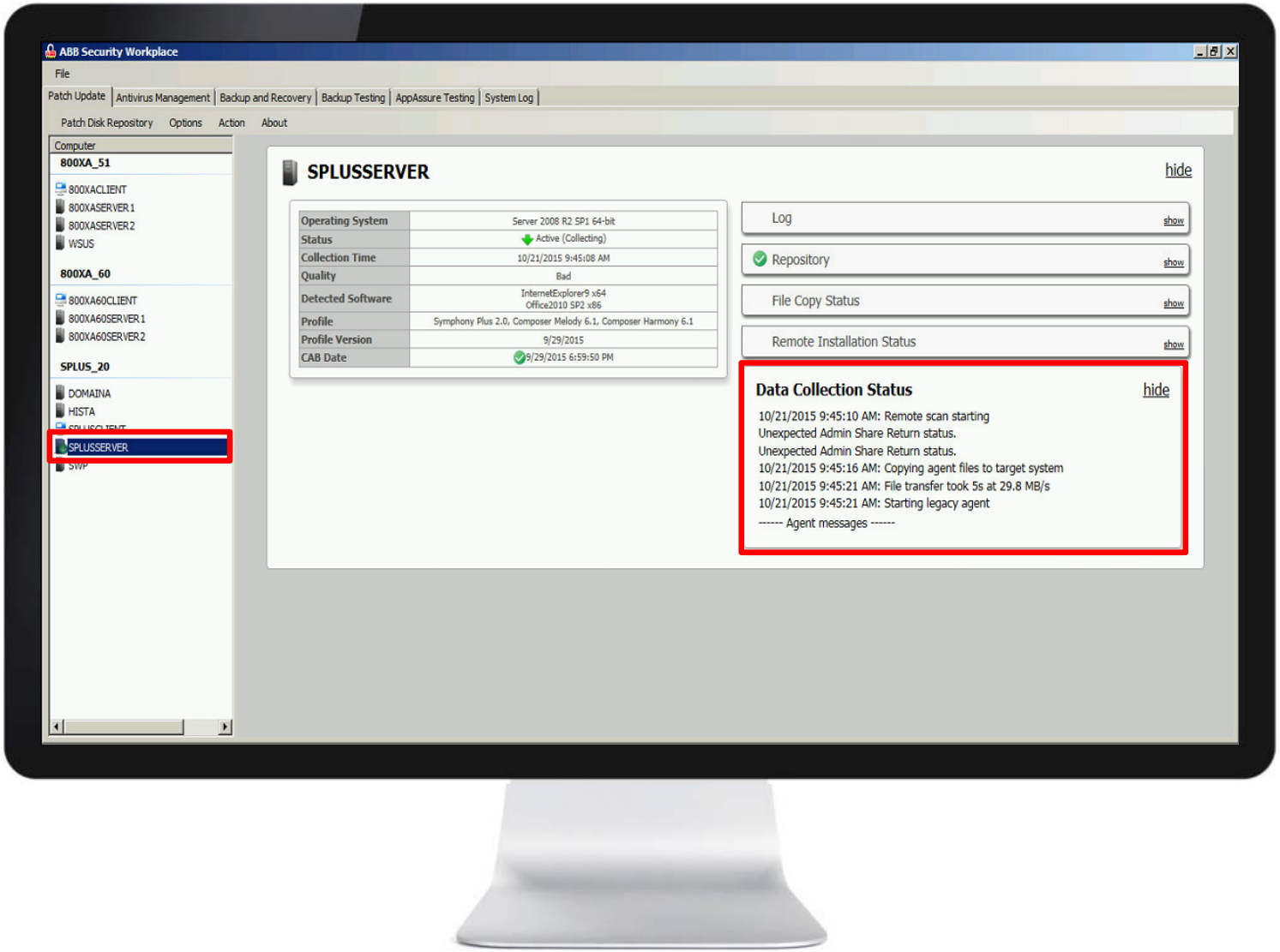


ABB Security Workplace
Maintain - Demonstration

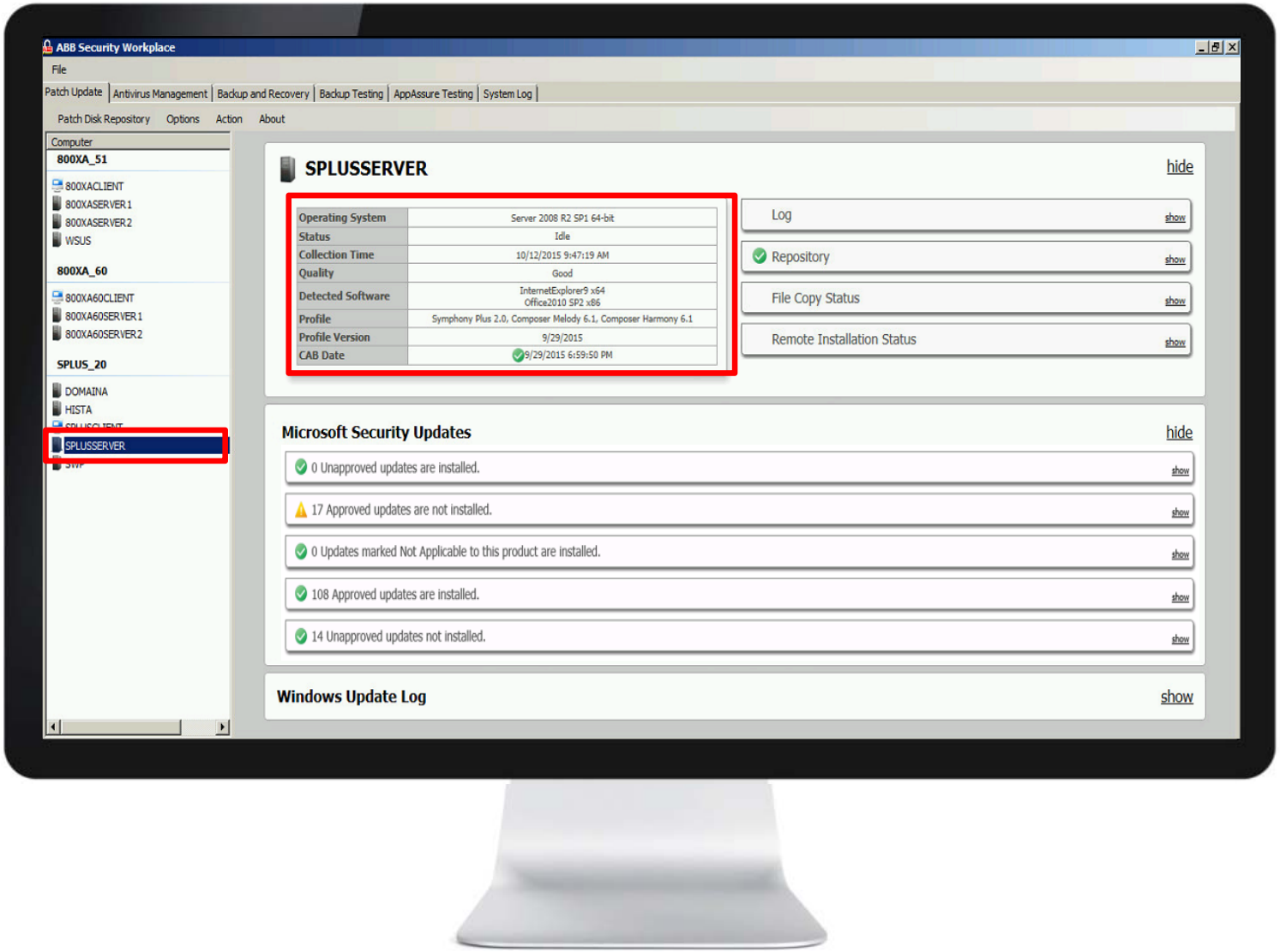


ABB Security Workplace
Maintain - Demonstration

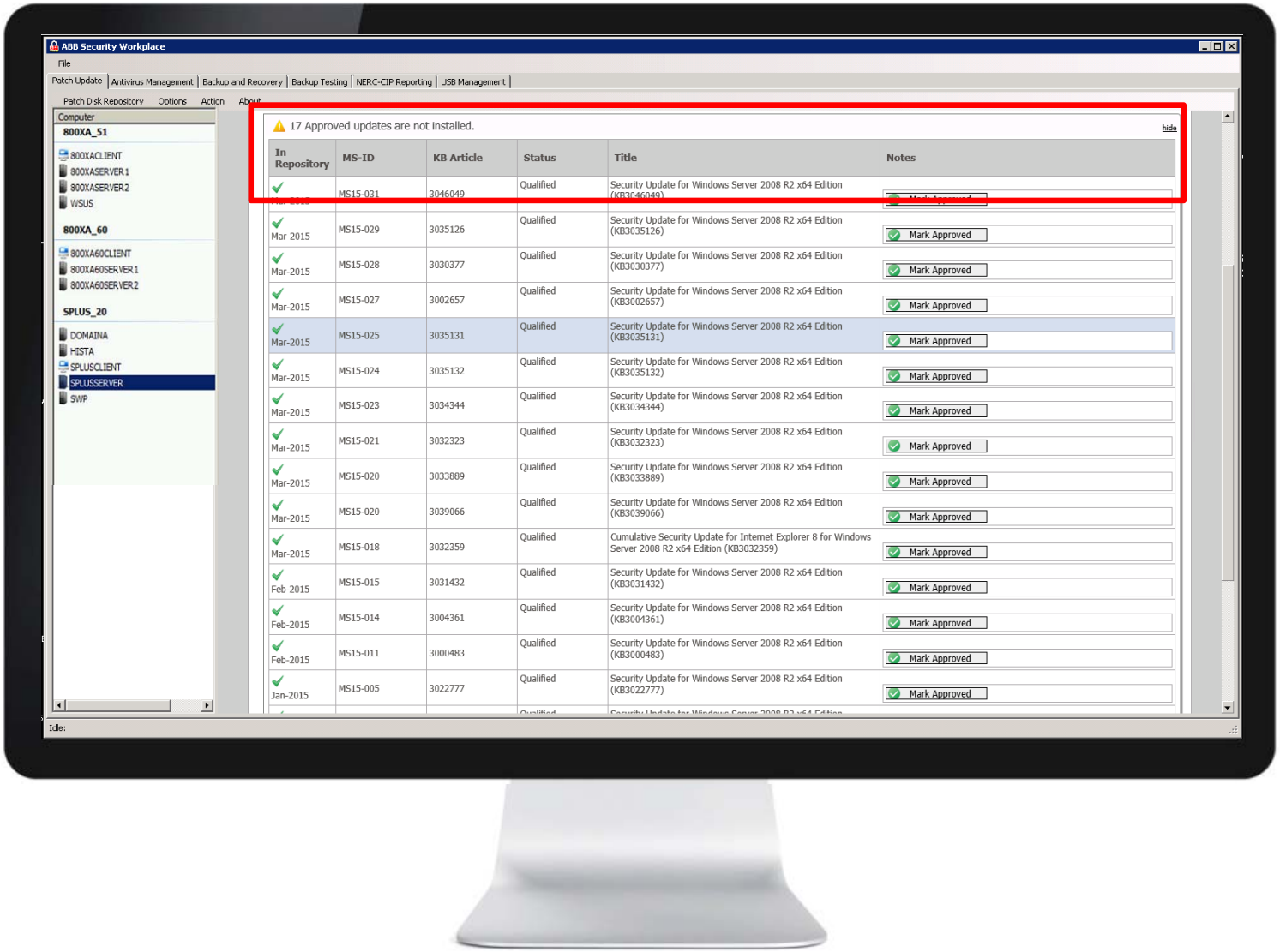


ABB Security Workplace
Maintain - Demonstration

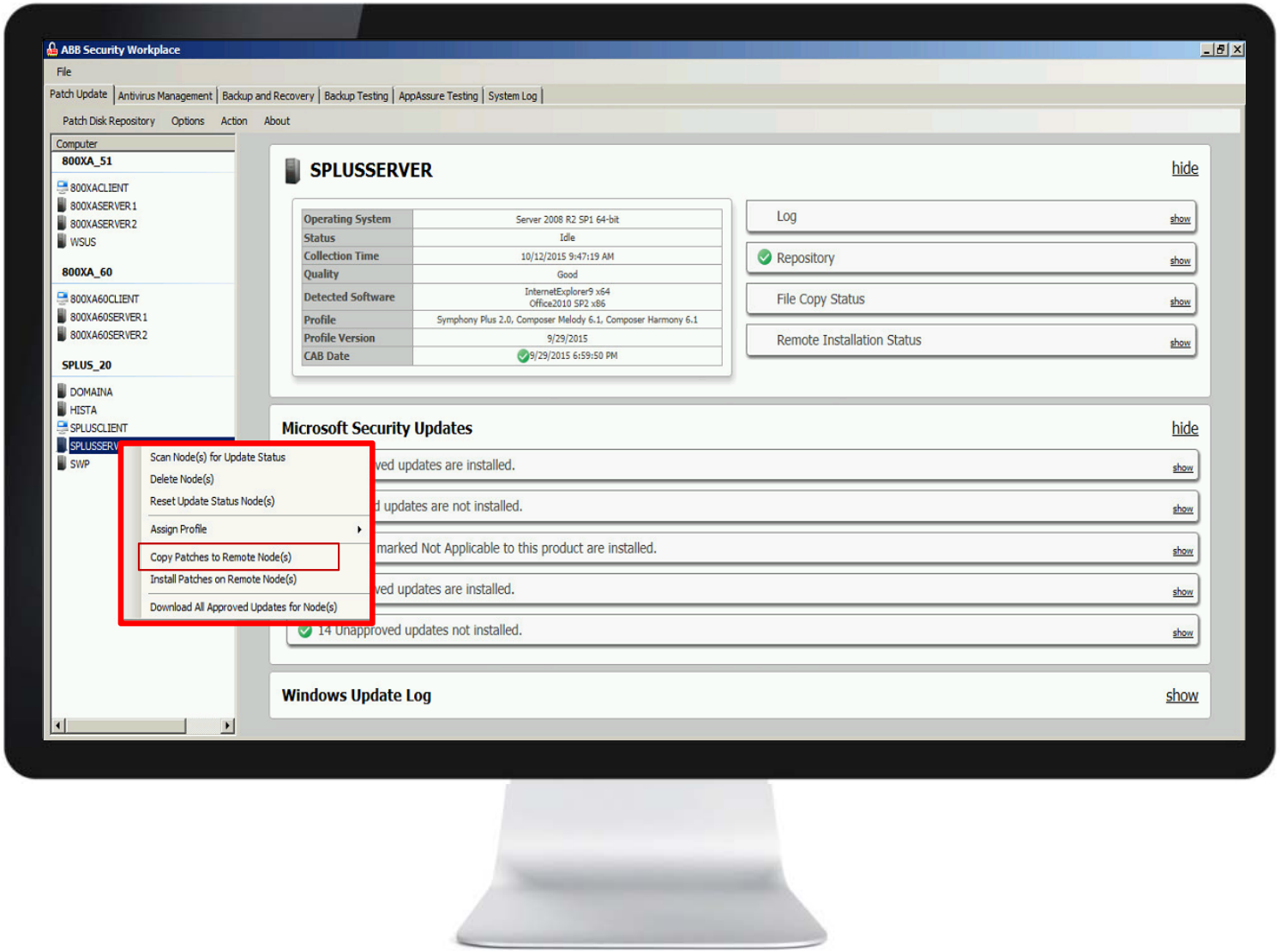


ABB Security Workplace
Maintain - Demonstration

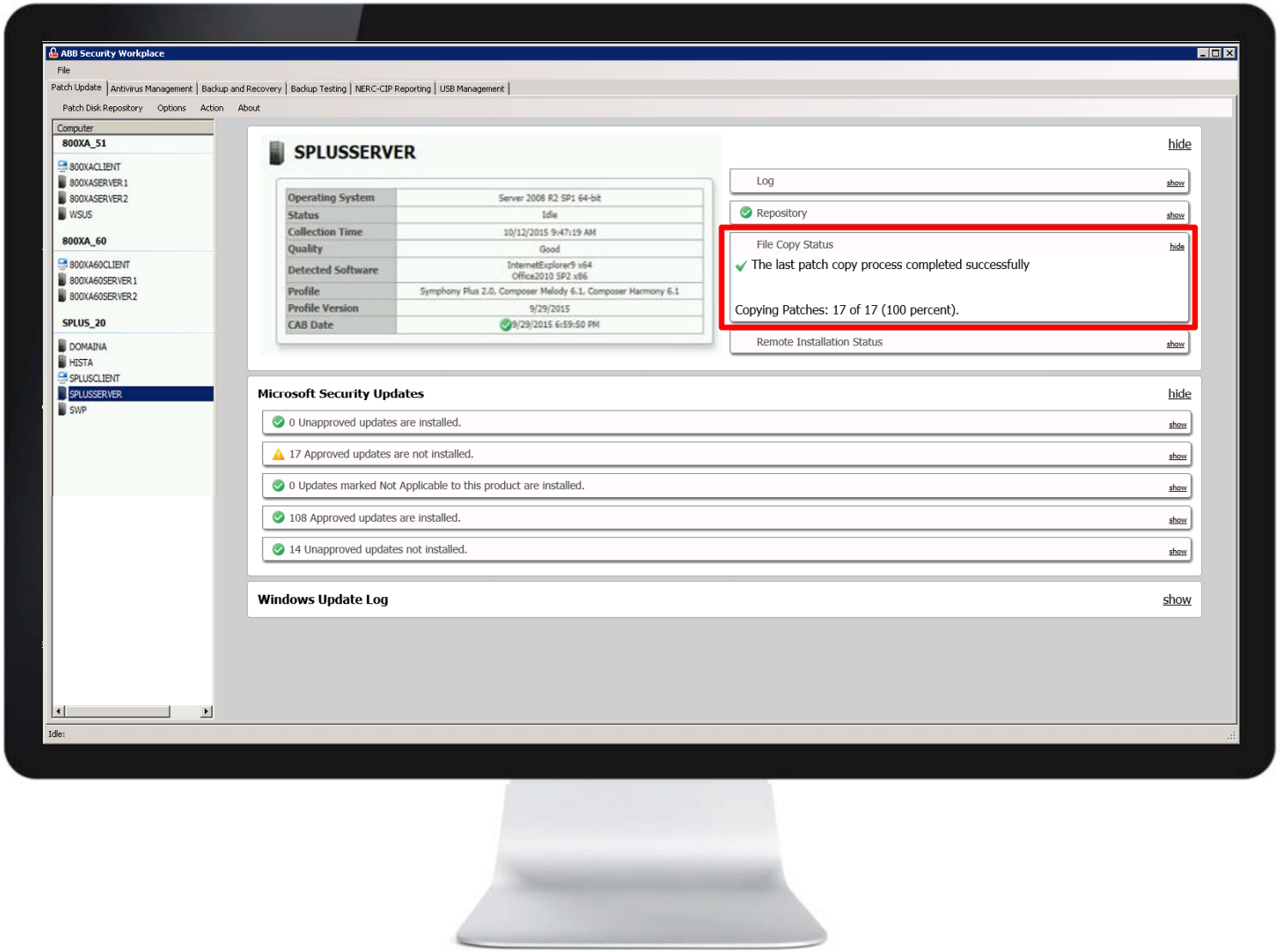


ABB Security Workplace
Maintain - Demonstration

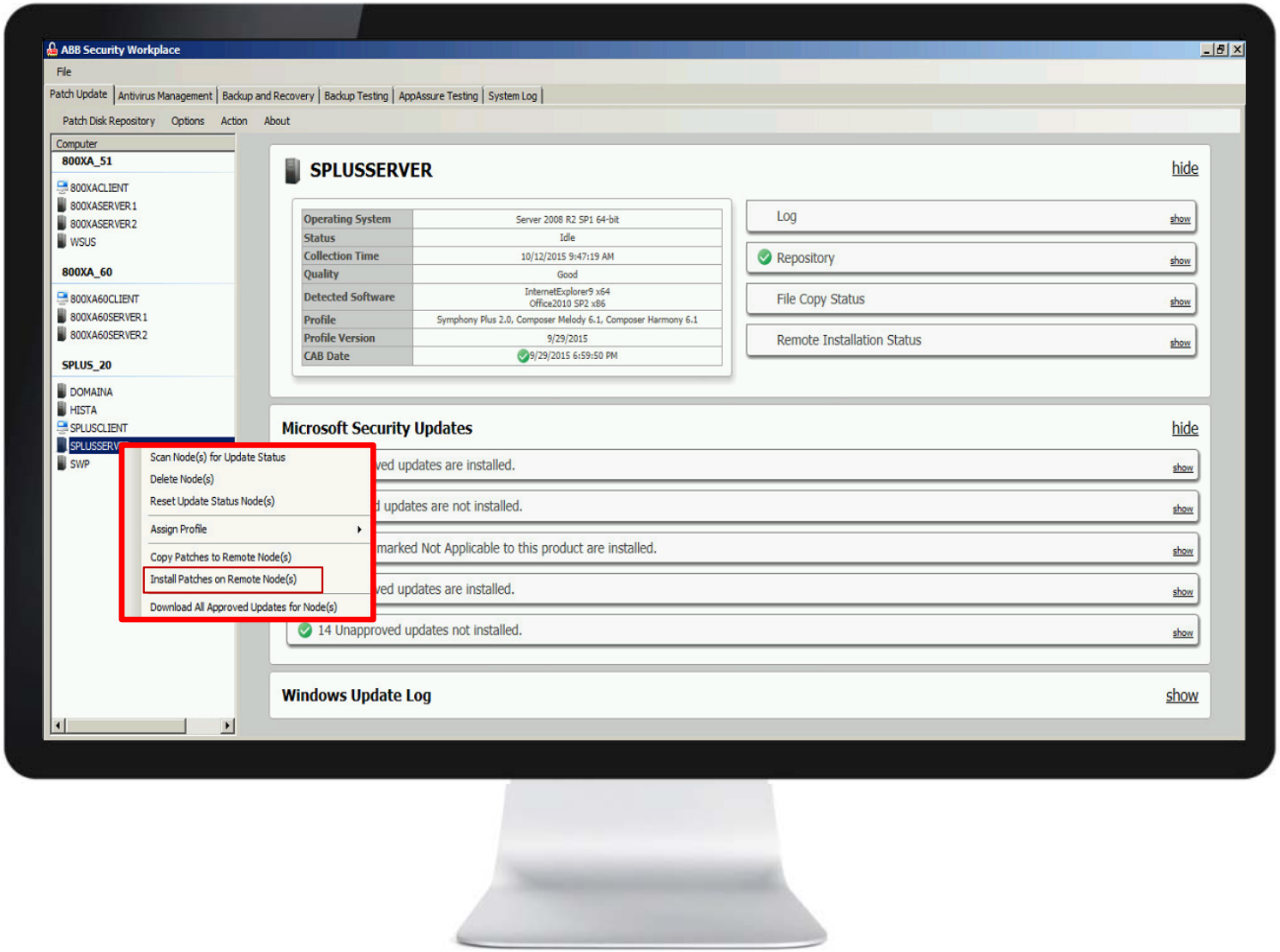


ABB Security Workplace
Maintain - Demonstration

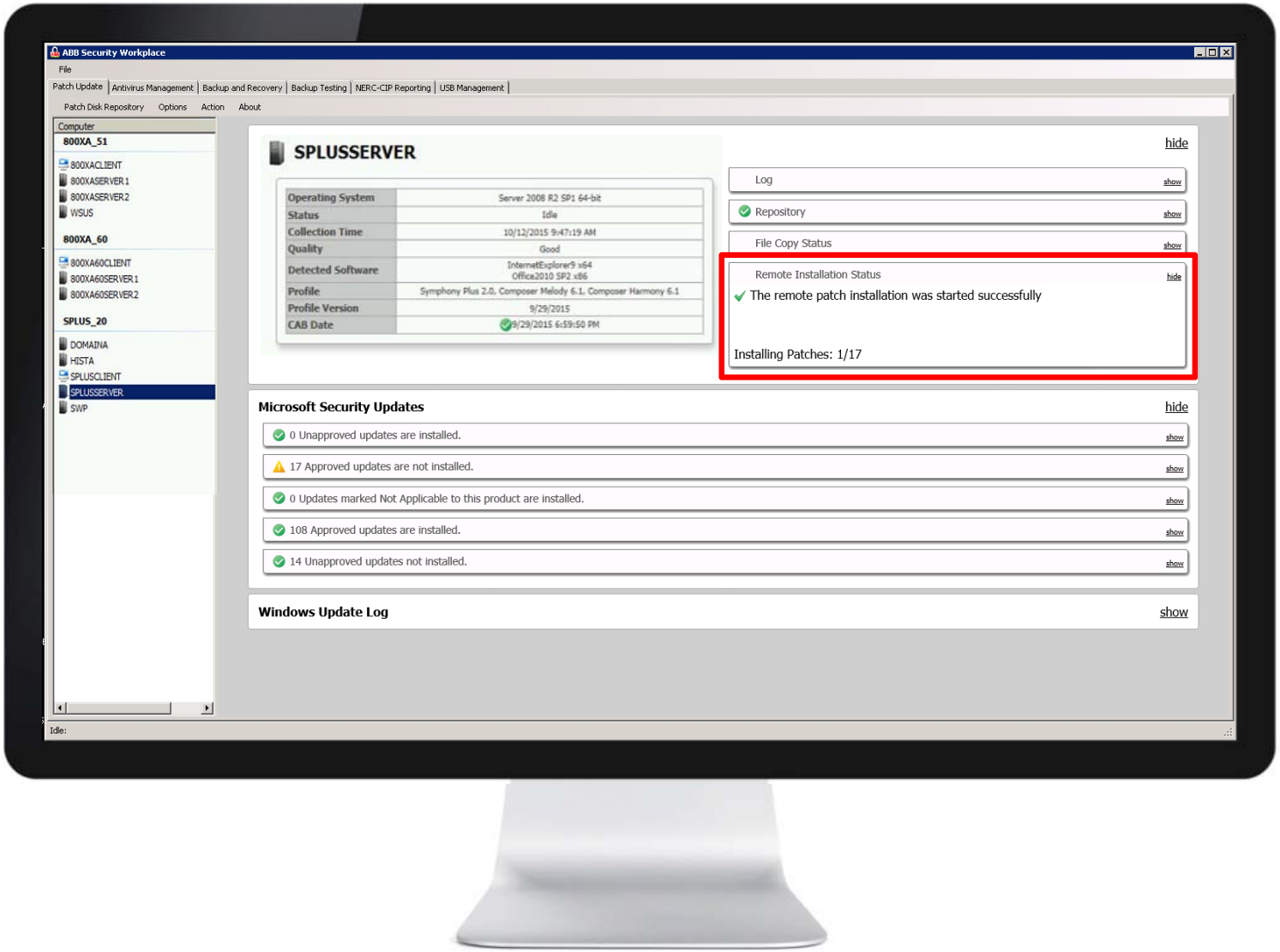


ABB Security Workplace
Maintain - Demonstration

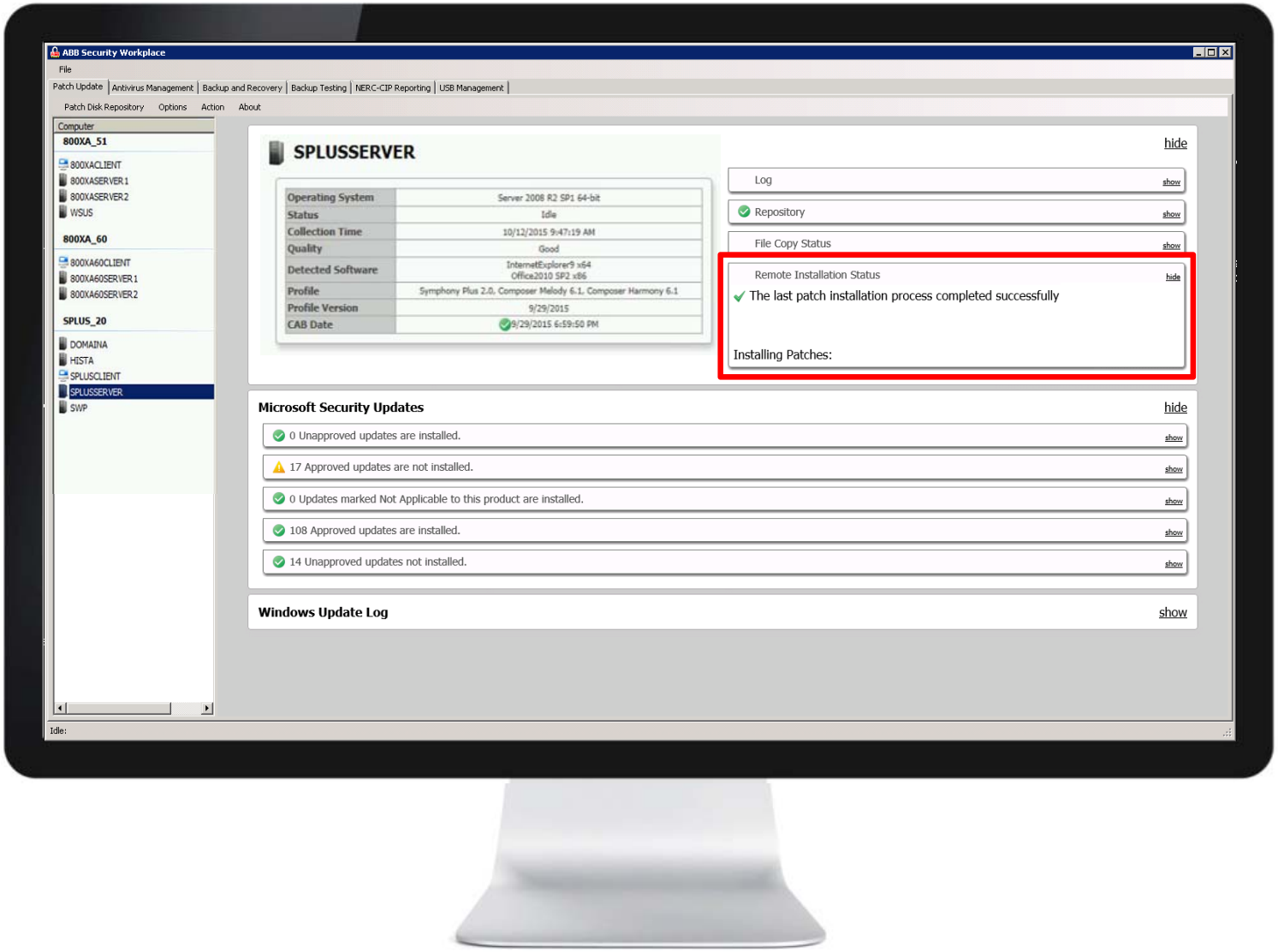


ABB Security Workplace
Maintain - Demonstration

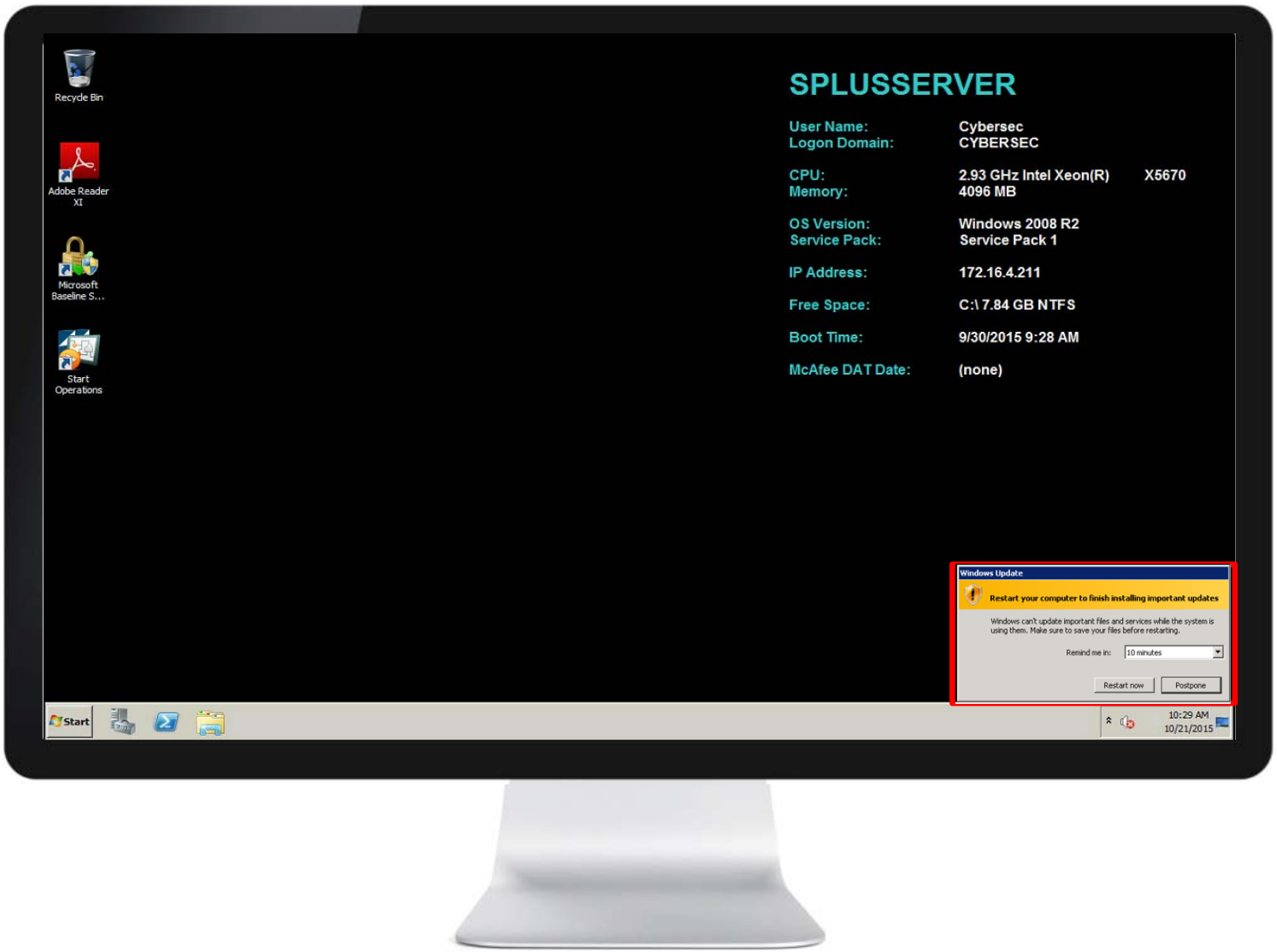


ABB Security Workplace
Maintain - Demonstration

ABB Security Workplace
Maintain - Demonstration

ABB Security Workplace
Maintain - Demonstration

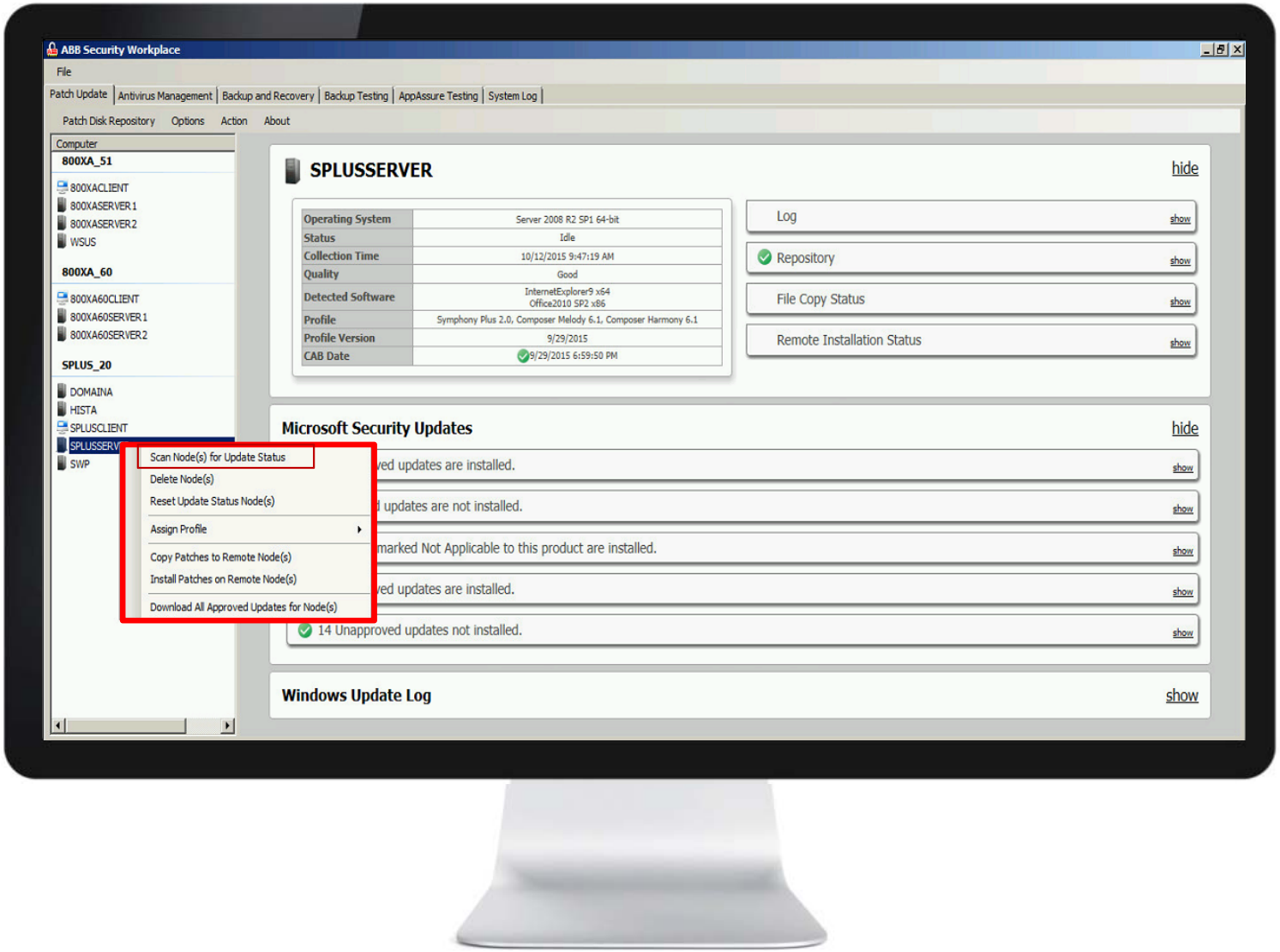


ABB Security Workplace
Maintain - Demonstration

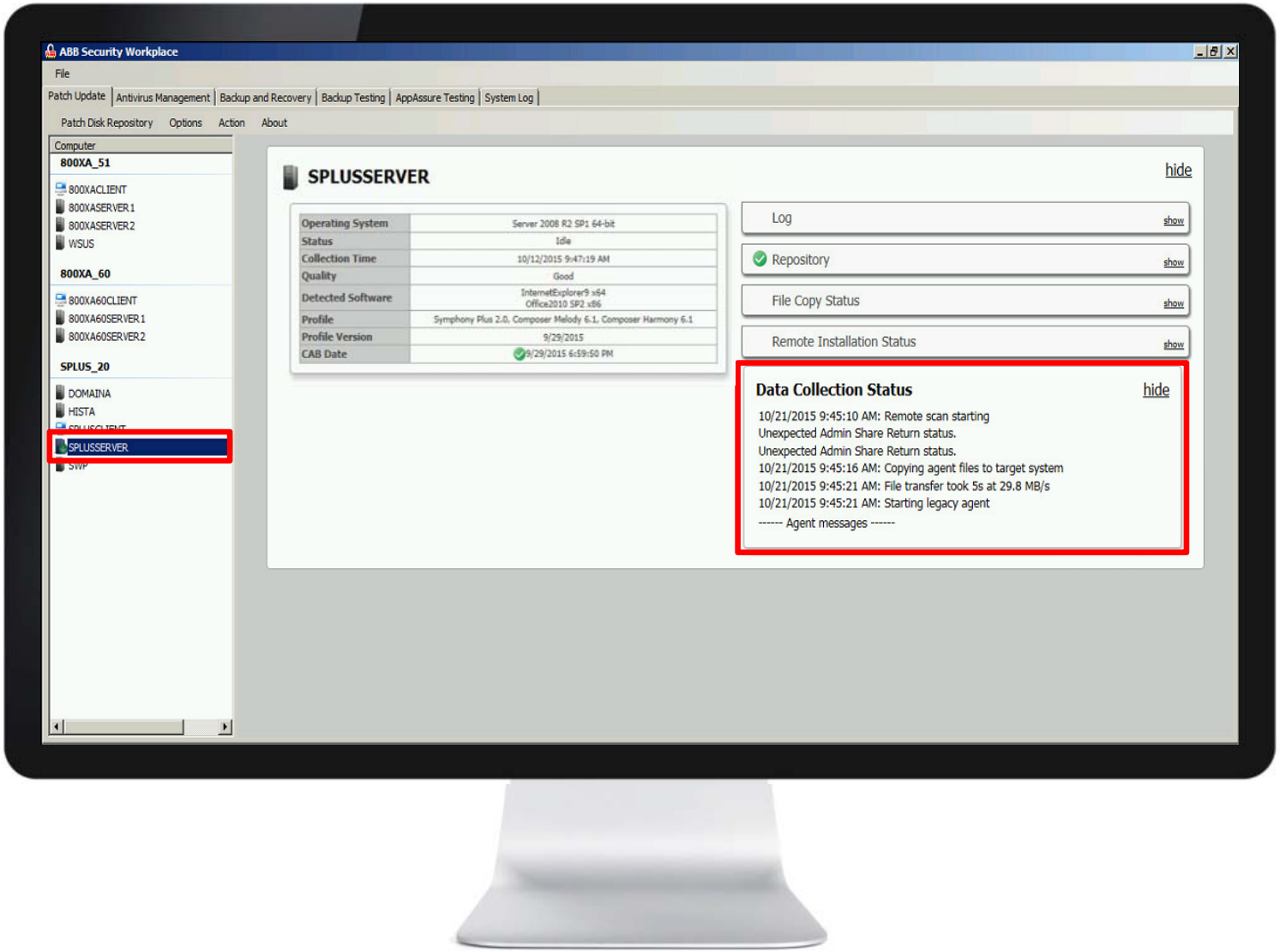


ABB Security Workplace
Maintain - Demonstration

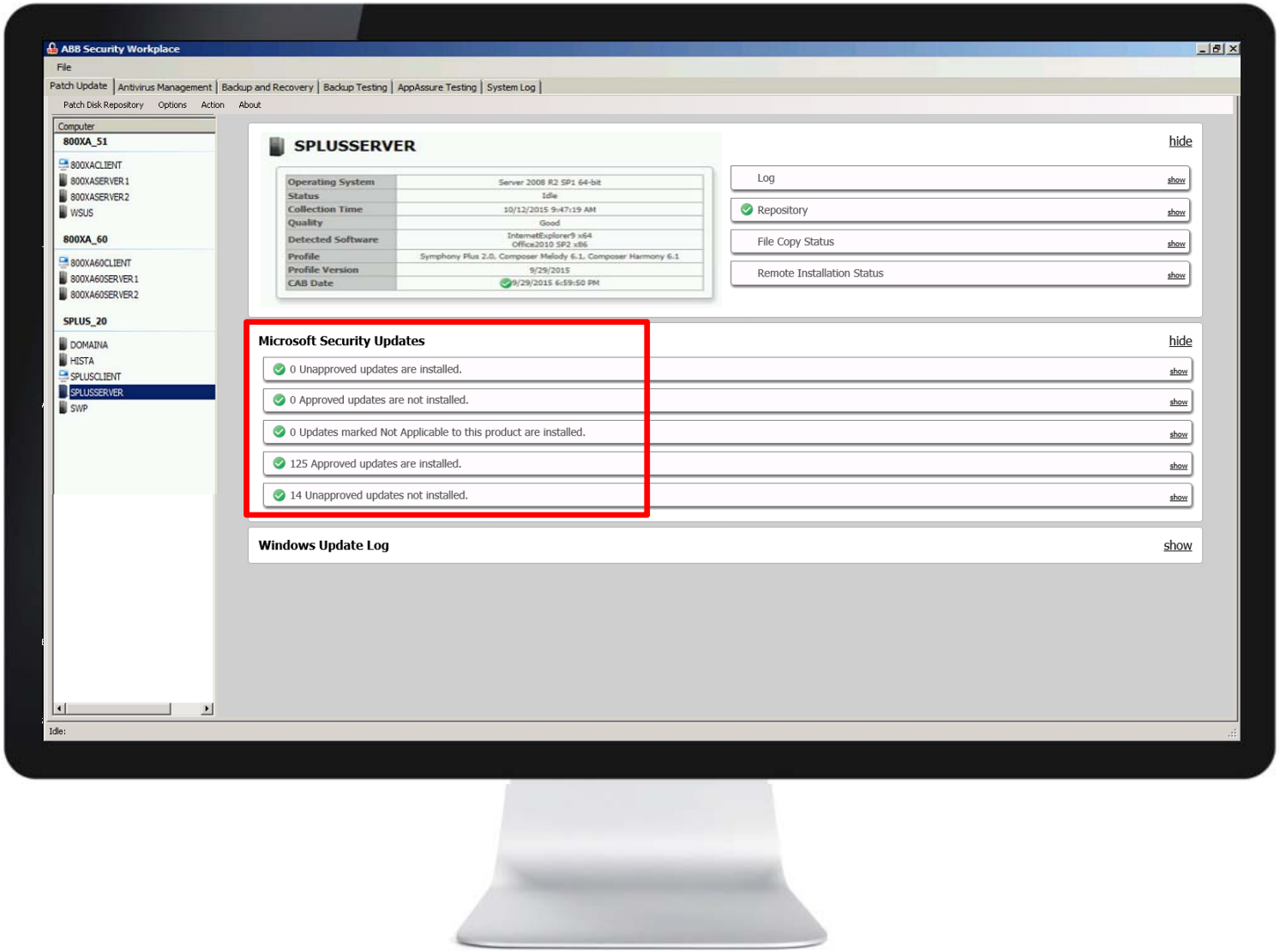


ABB Security Workplace
Maintain - Demonstration

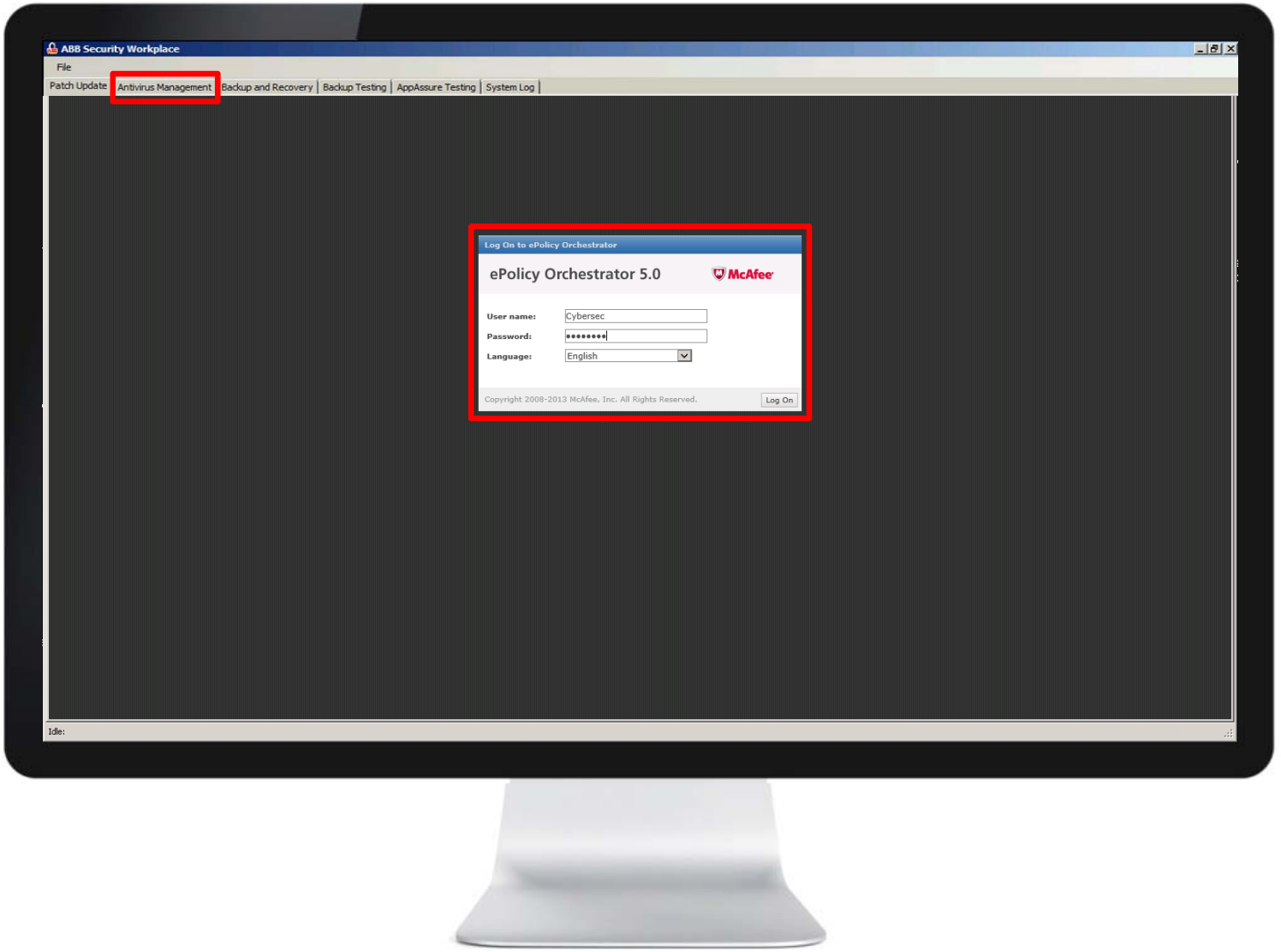


ABB Security Workplace
Maintain - Demonstration

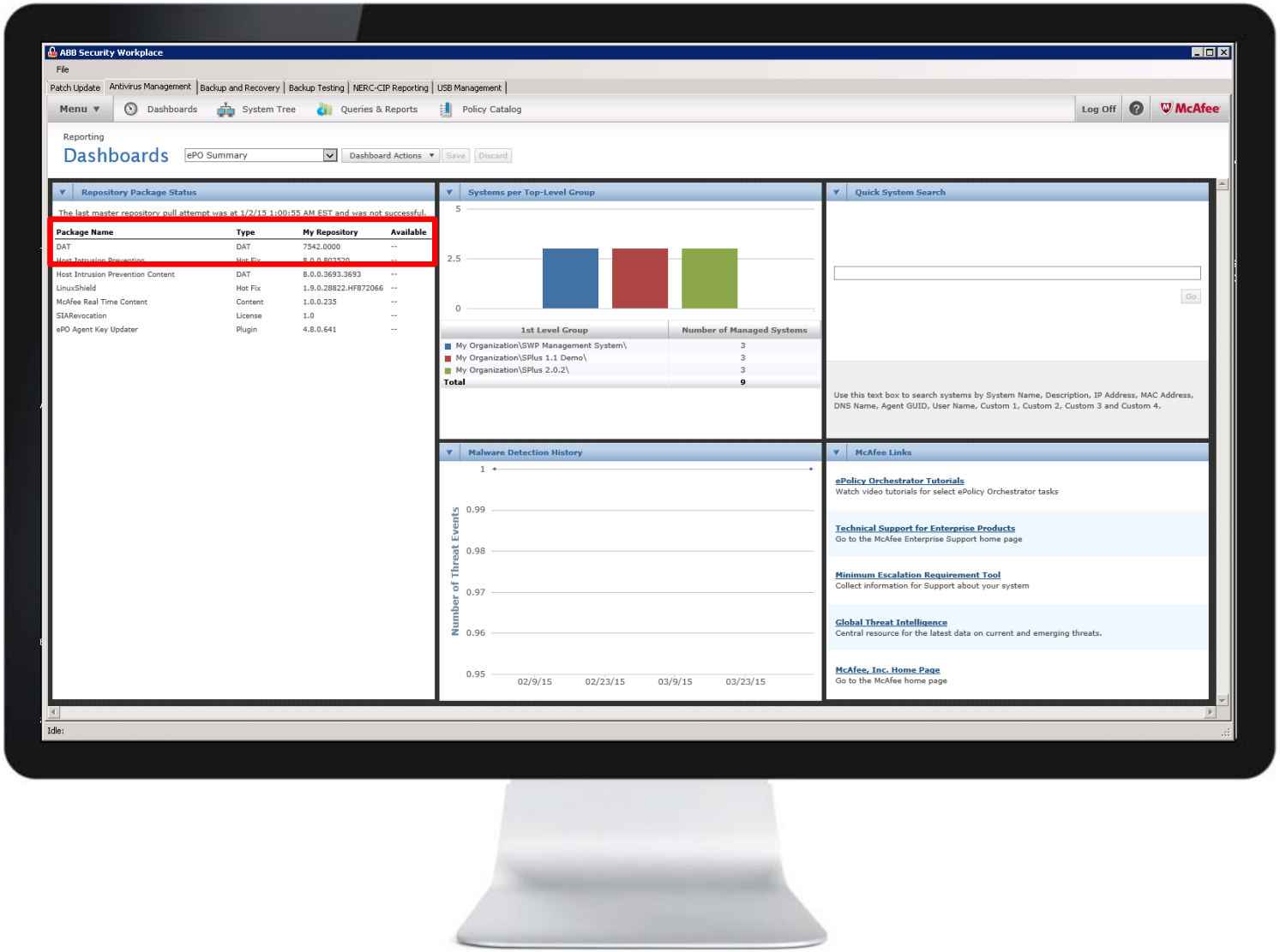


ABB Security Workplace
Maintain - Demonstration

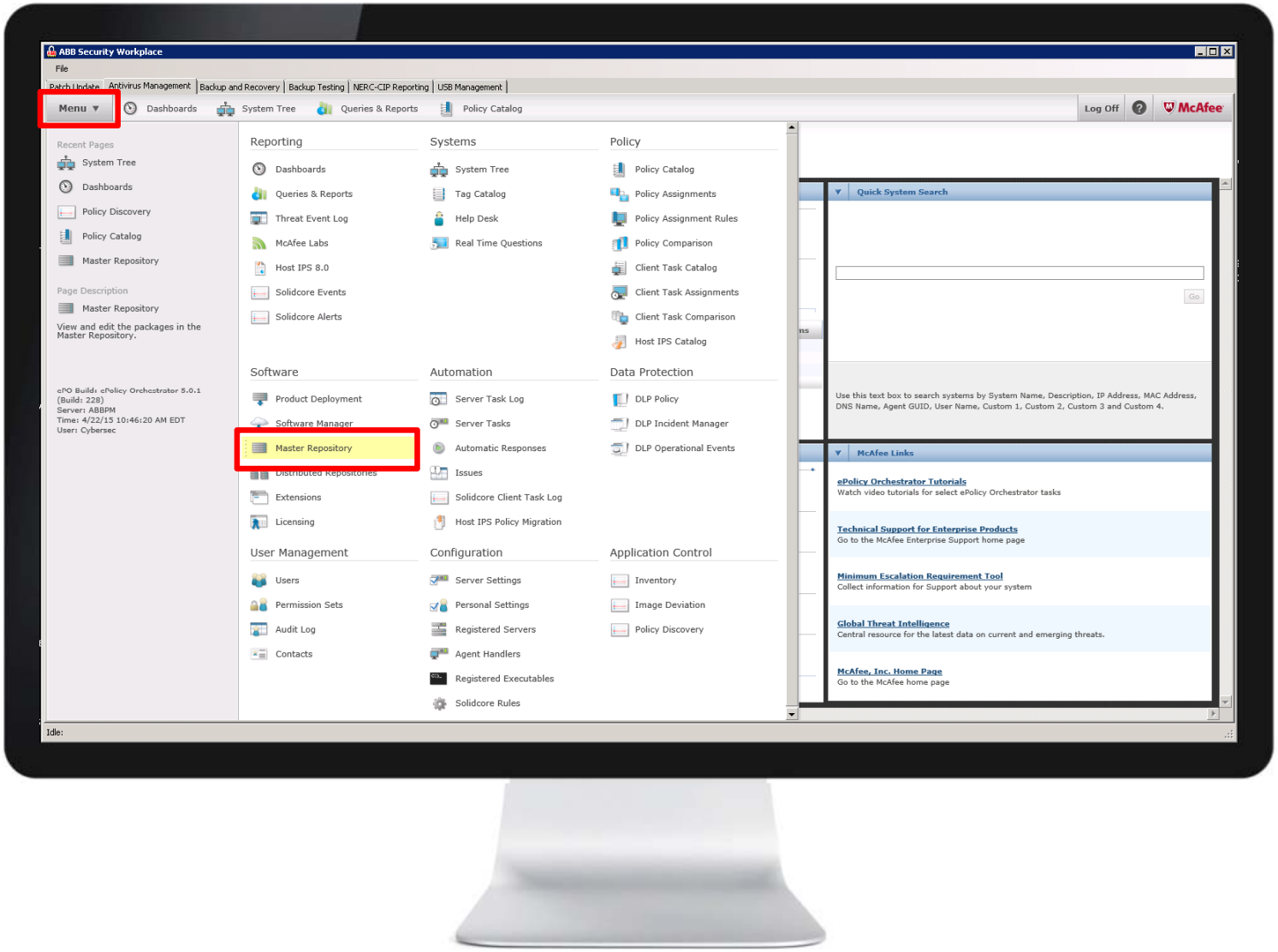


ABB Security Workplace
Maintain - Demonstration

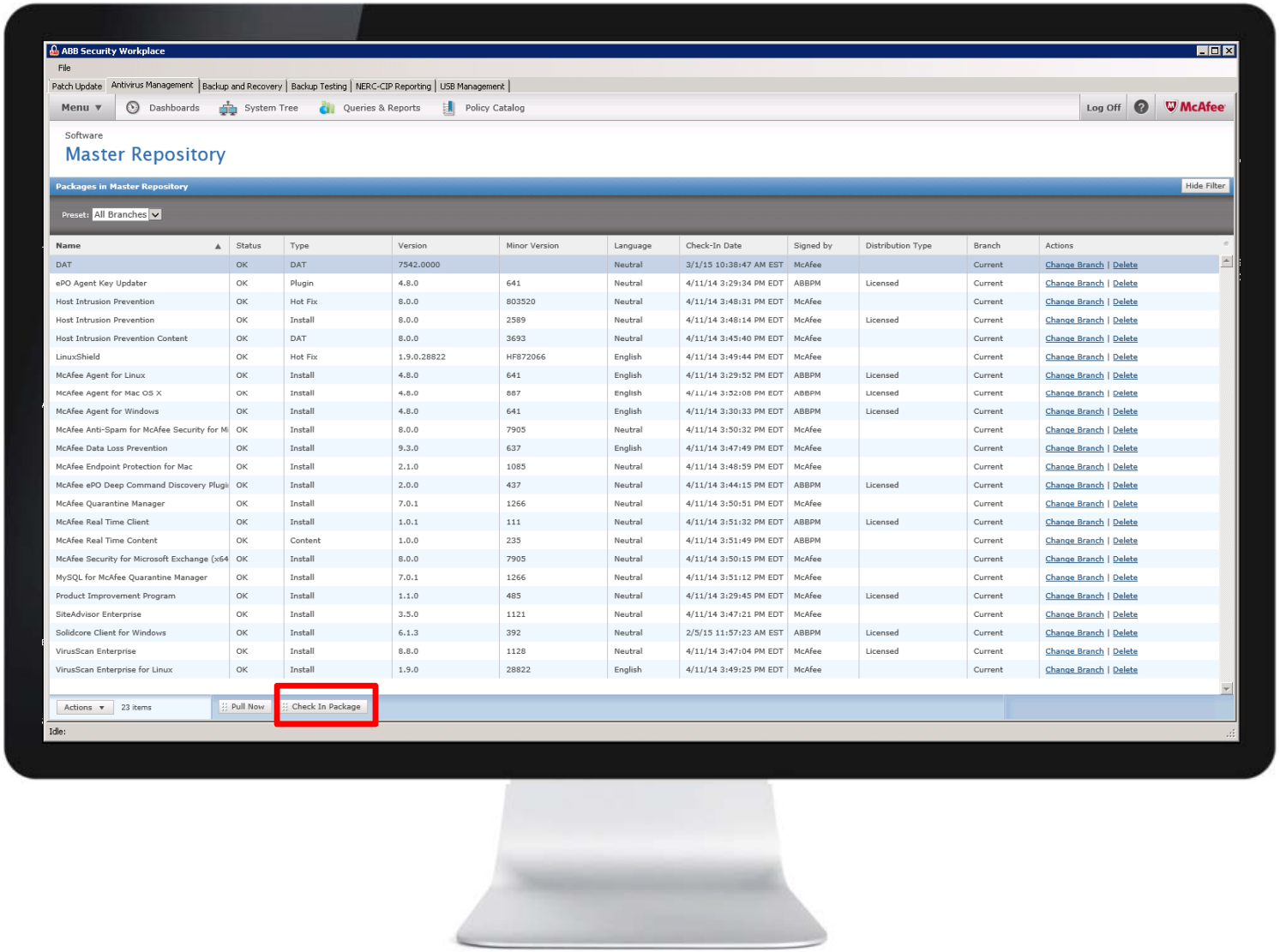


ABB Security Workplace
Maintain - Demonstration

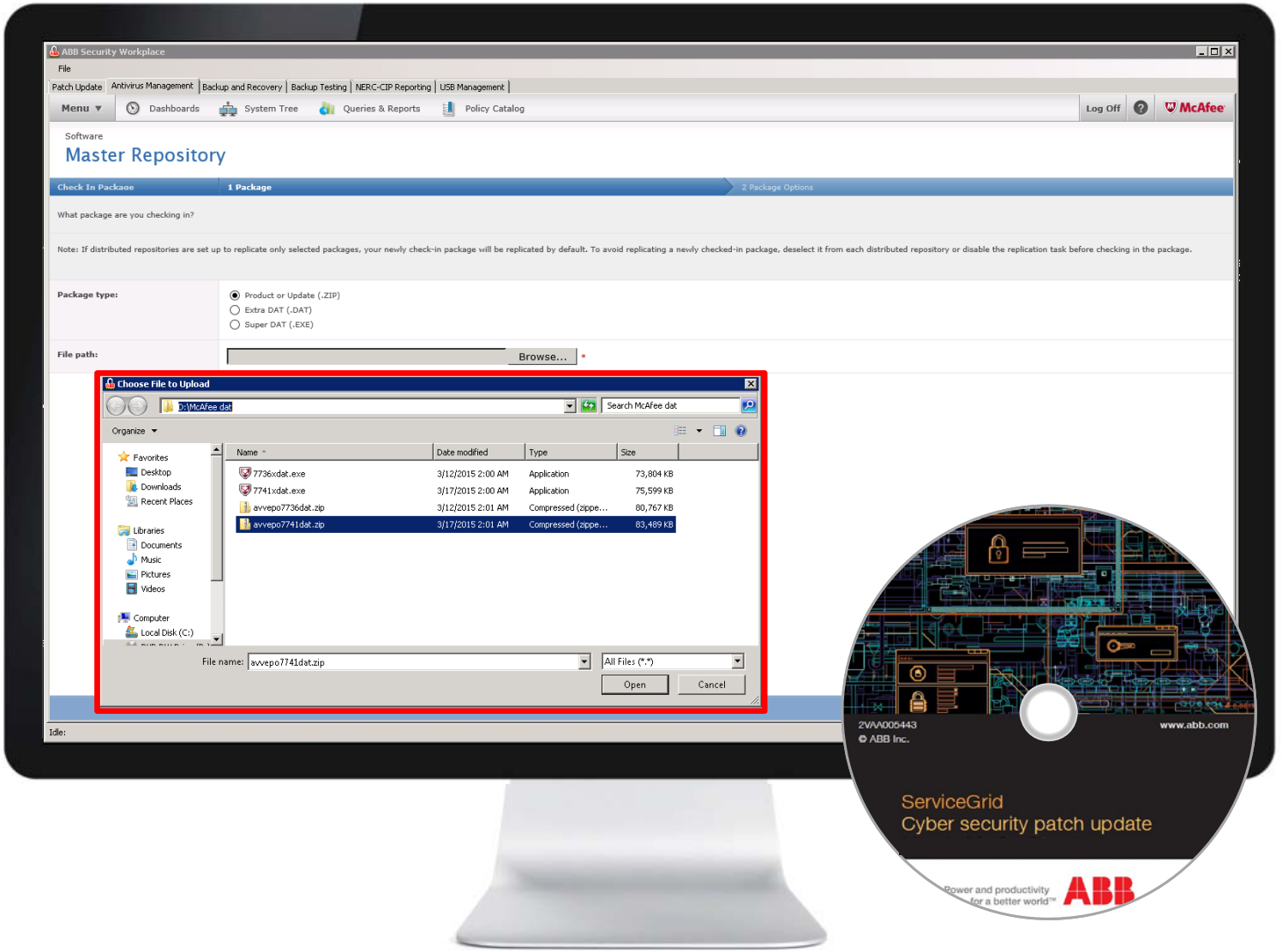


ABB Security Workplace
Maintain - Demonstration

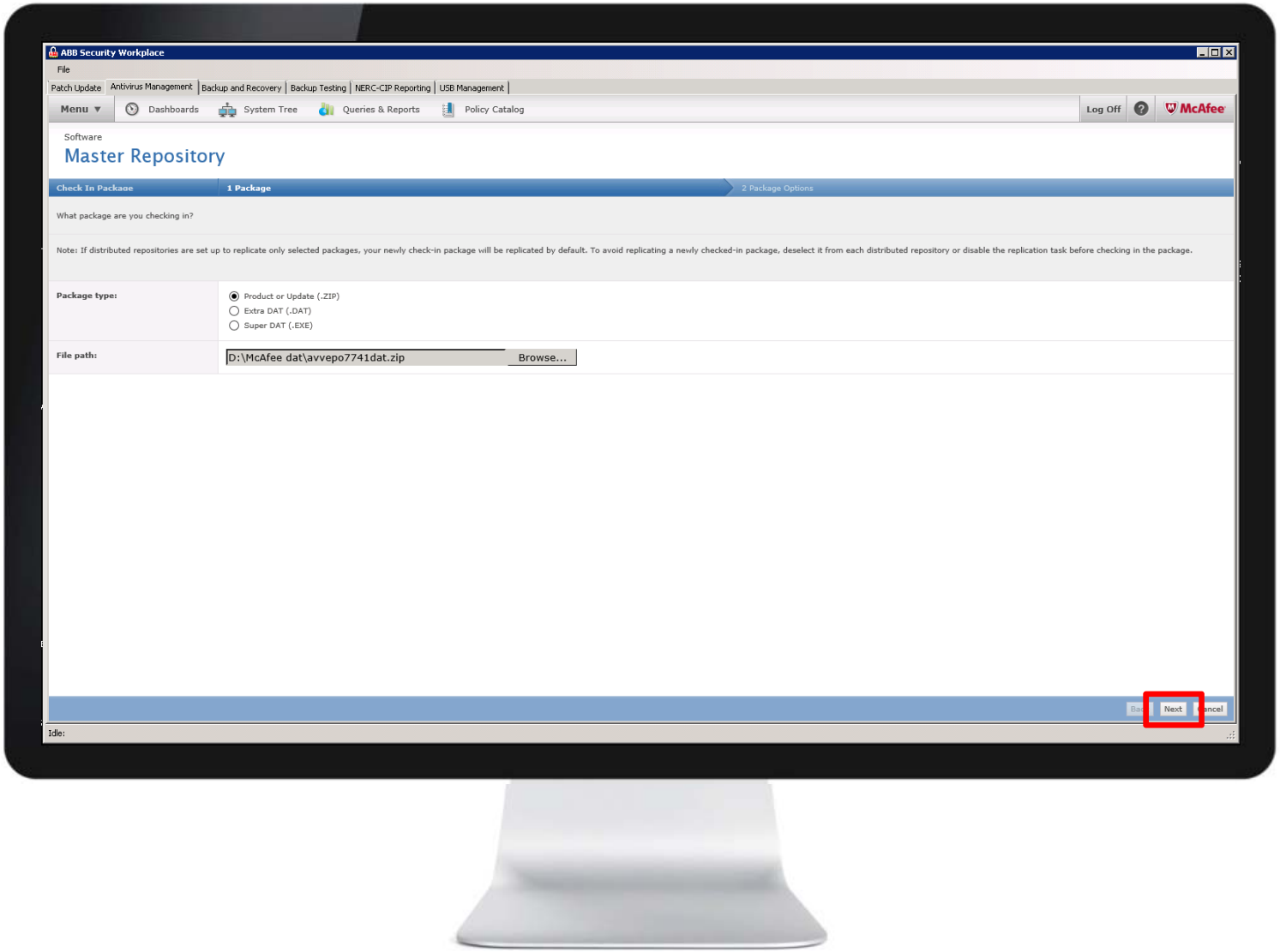


ABB Security Workplace
Maintain - Demonstration

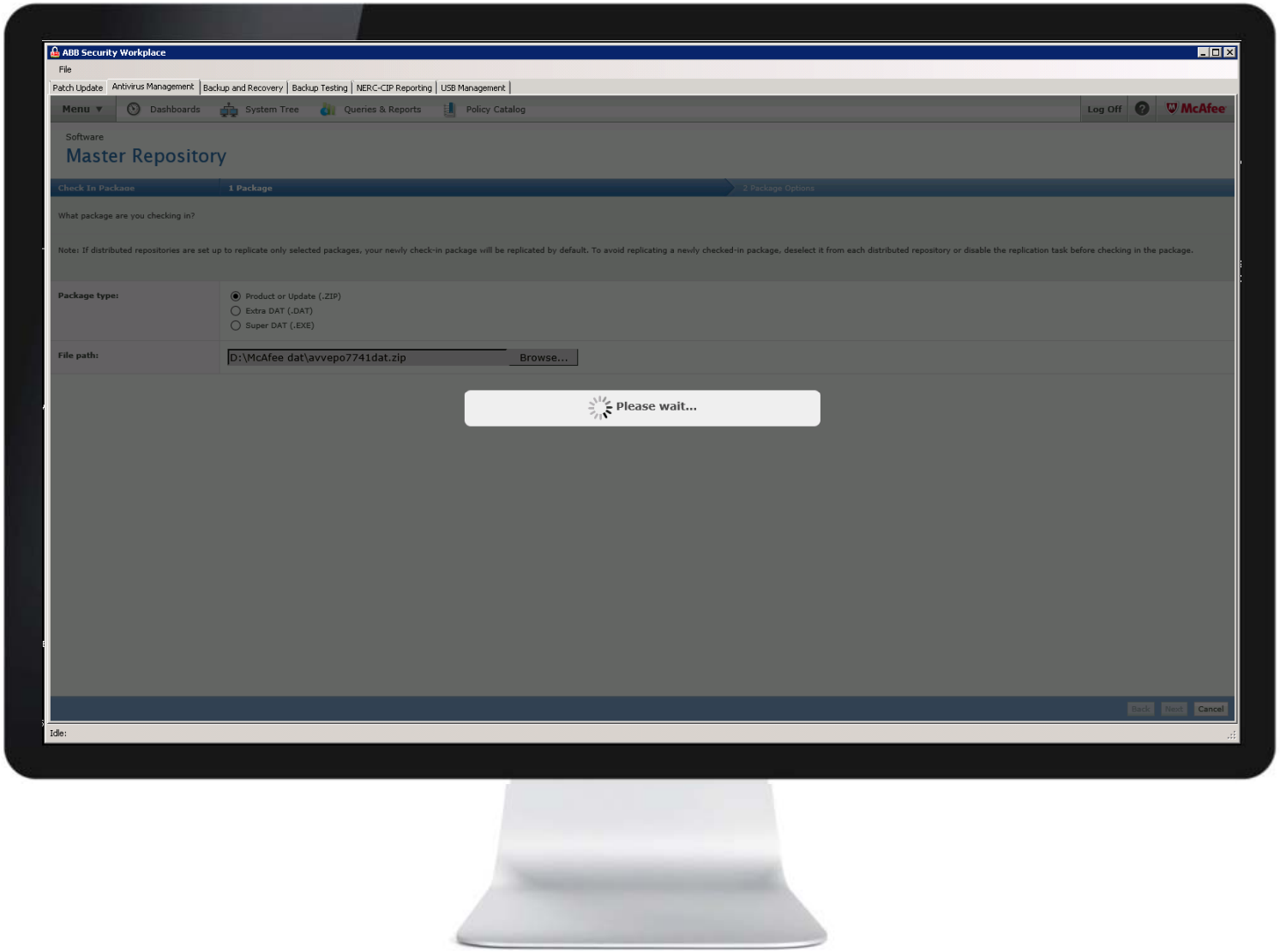


ABB Security Workplace
Maintain - Demonstration

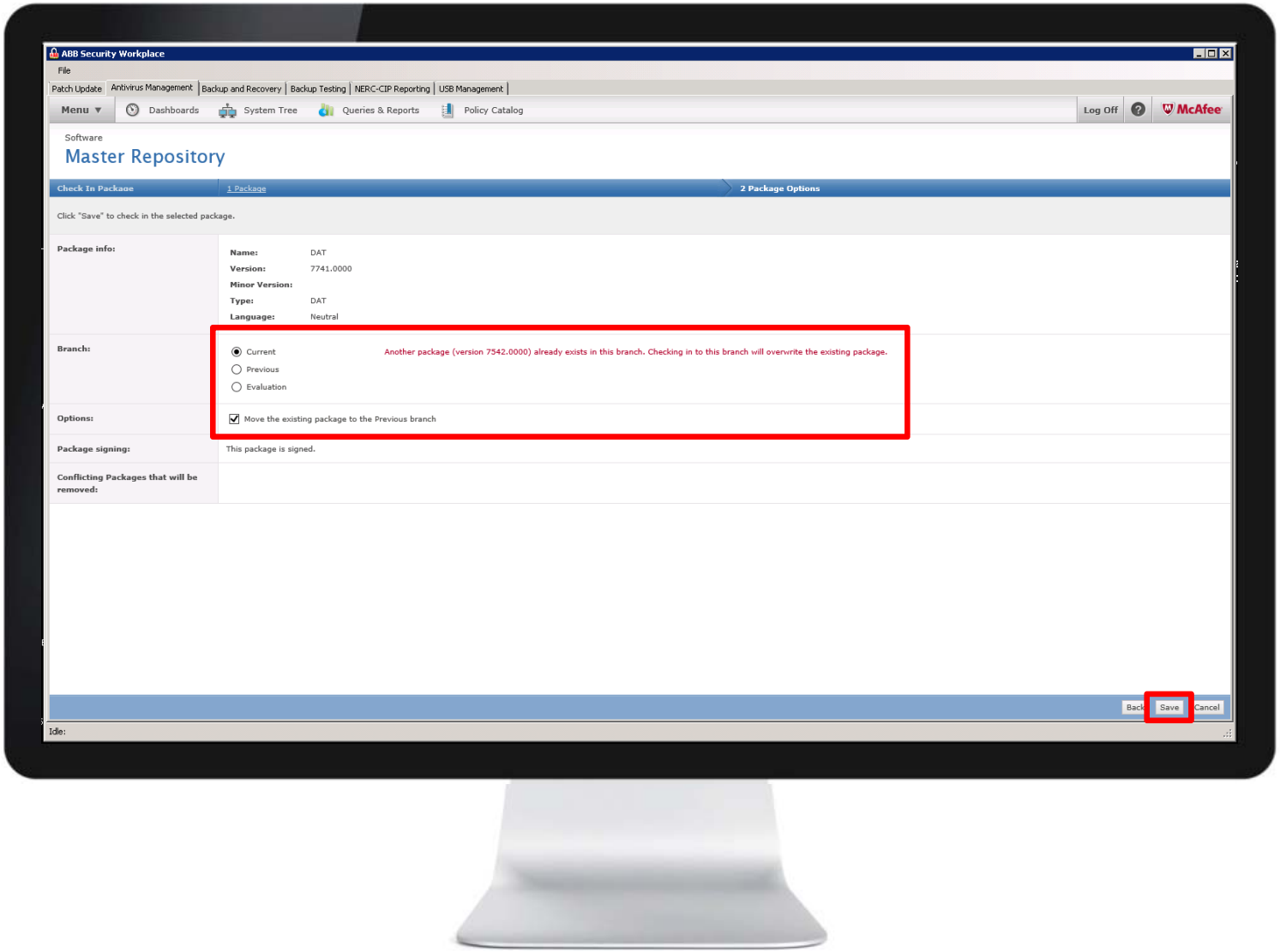


ABB Security Workplace
Maintain - Demonstration

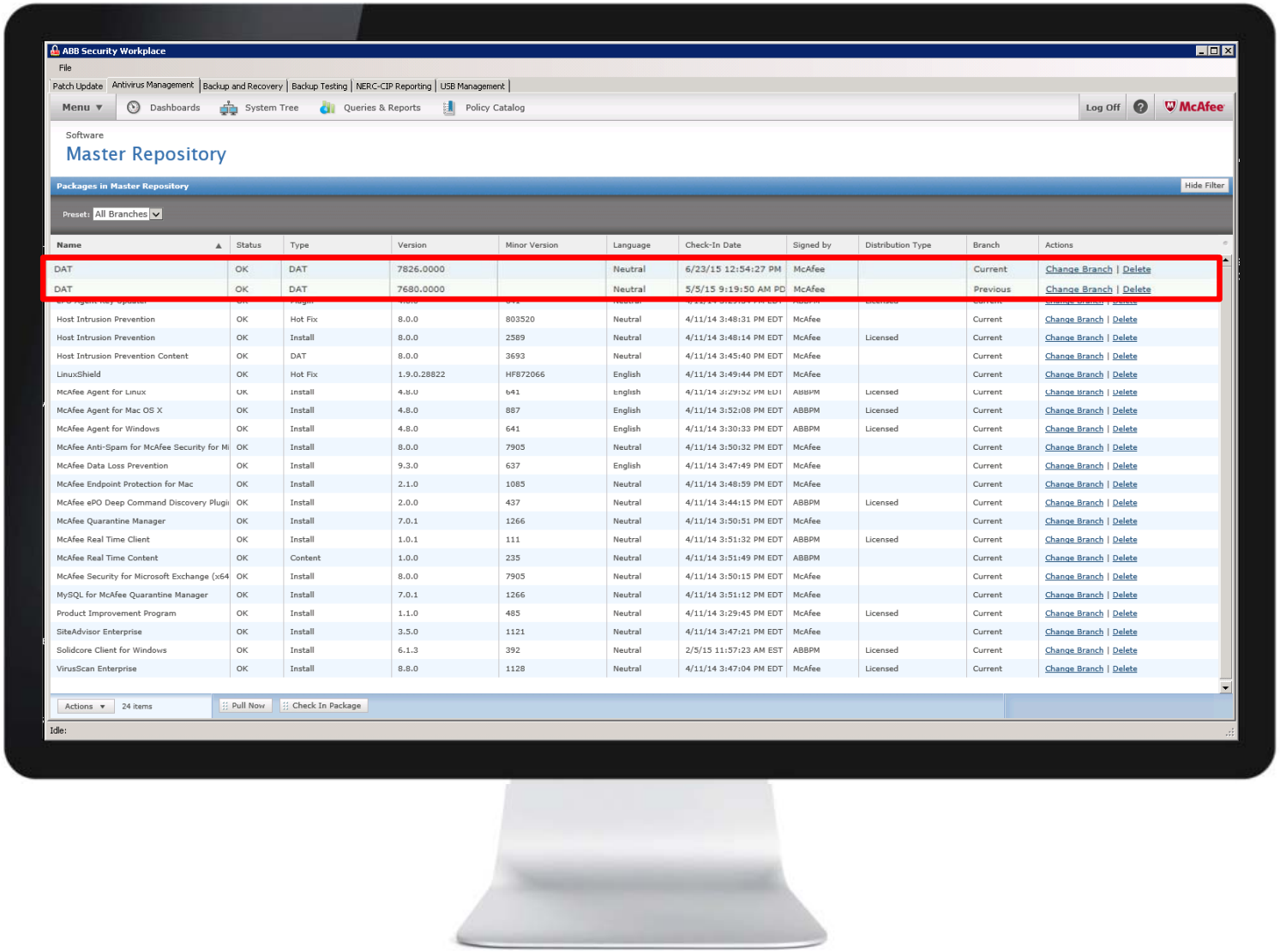


ABB Security Workplace
Maintain - Demonstration

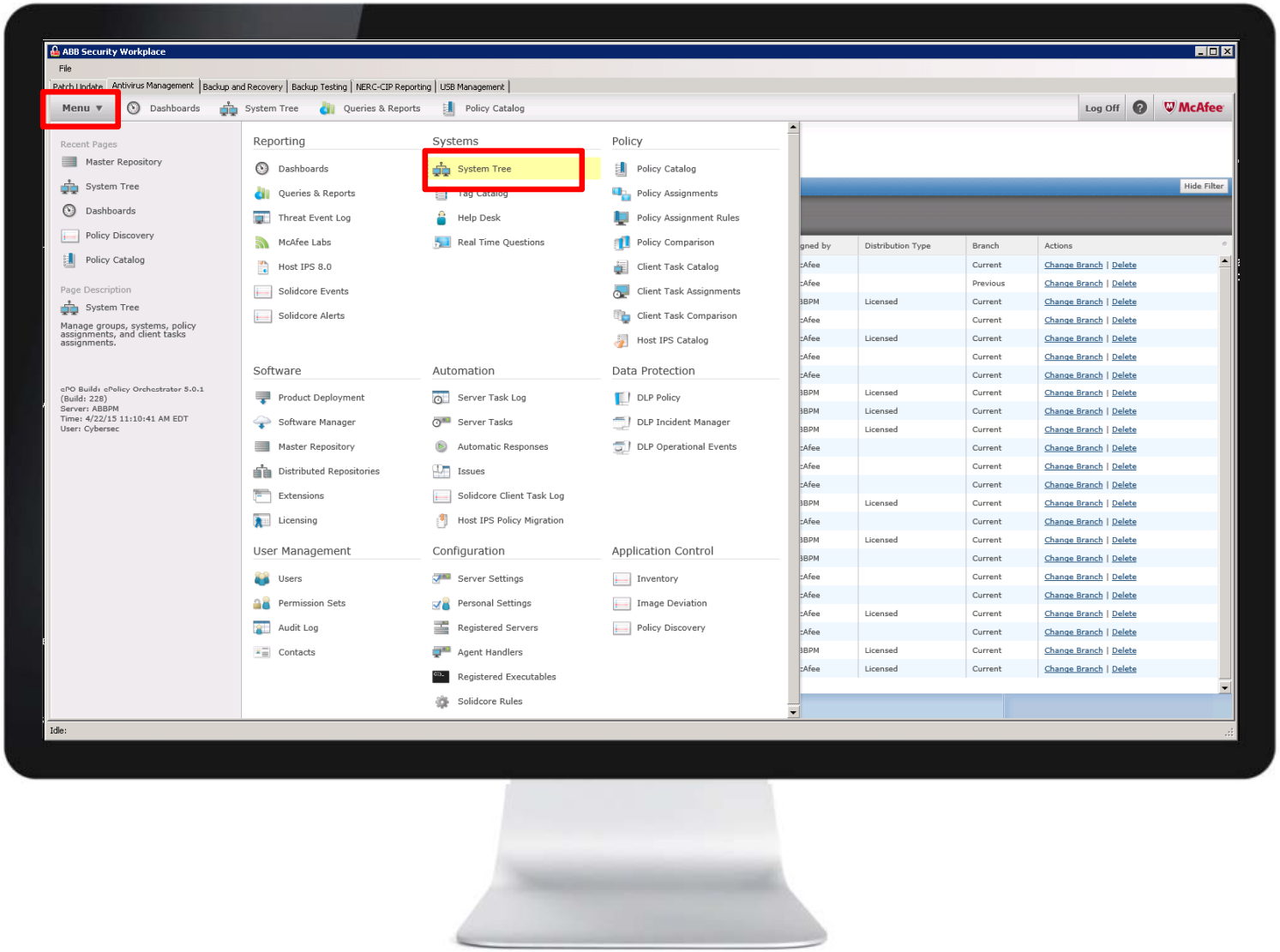


ABB Security Workplace
Maintain - Demonstration

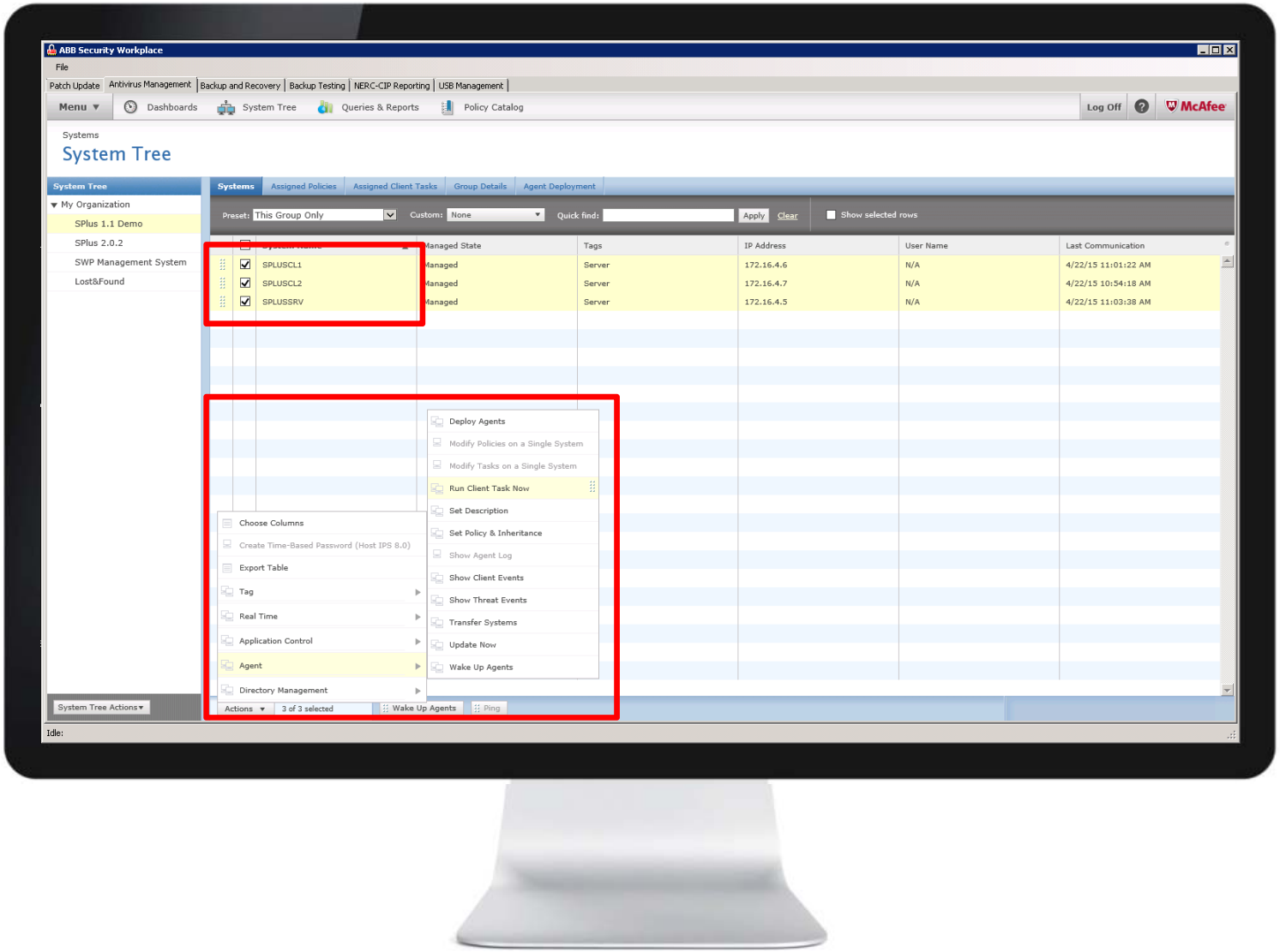


ABB Security Workplace
Maintain - Demonstration

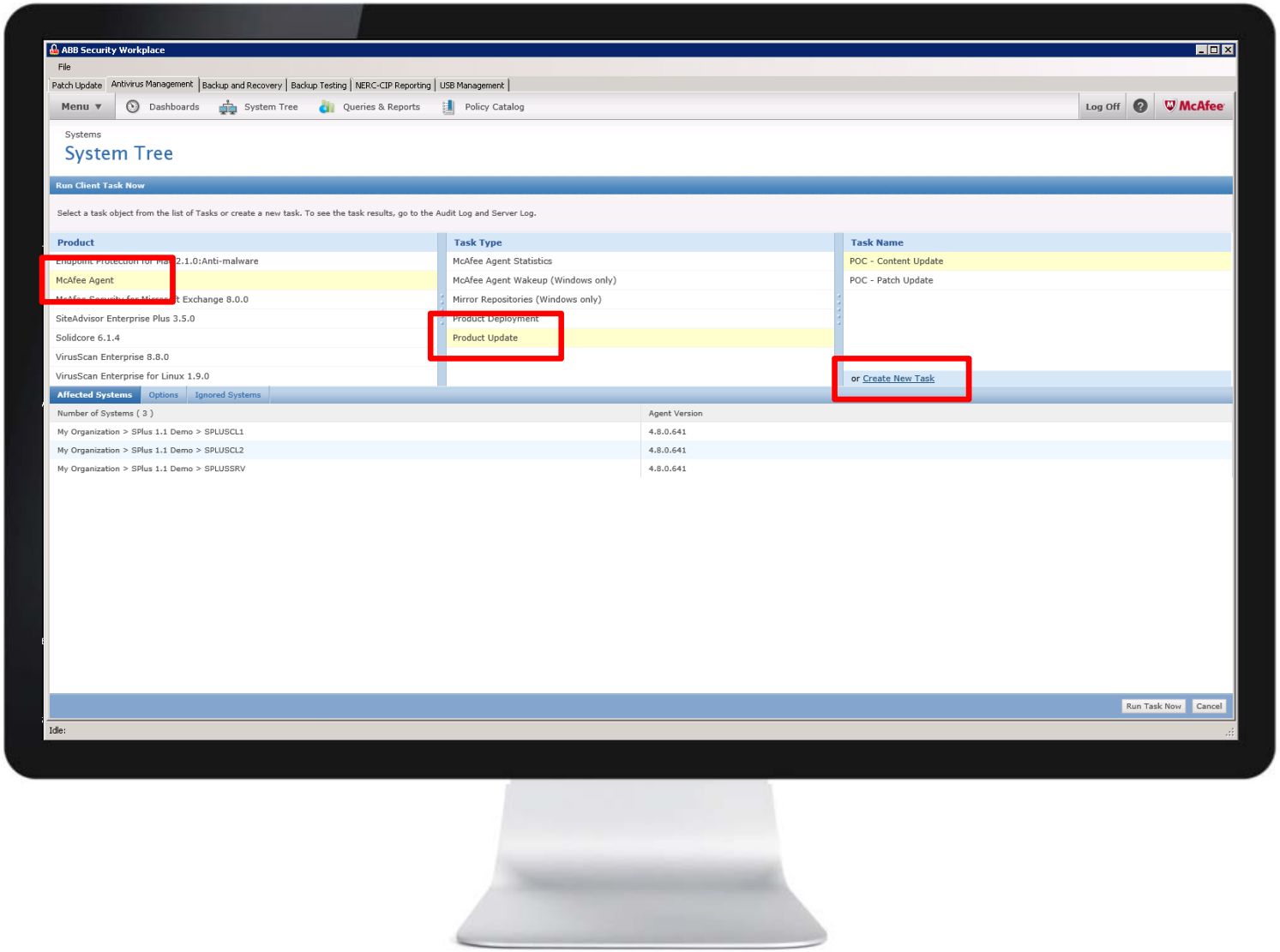


ABB Security Workplace
Maintain - Demonstration

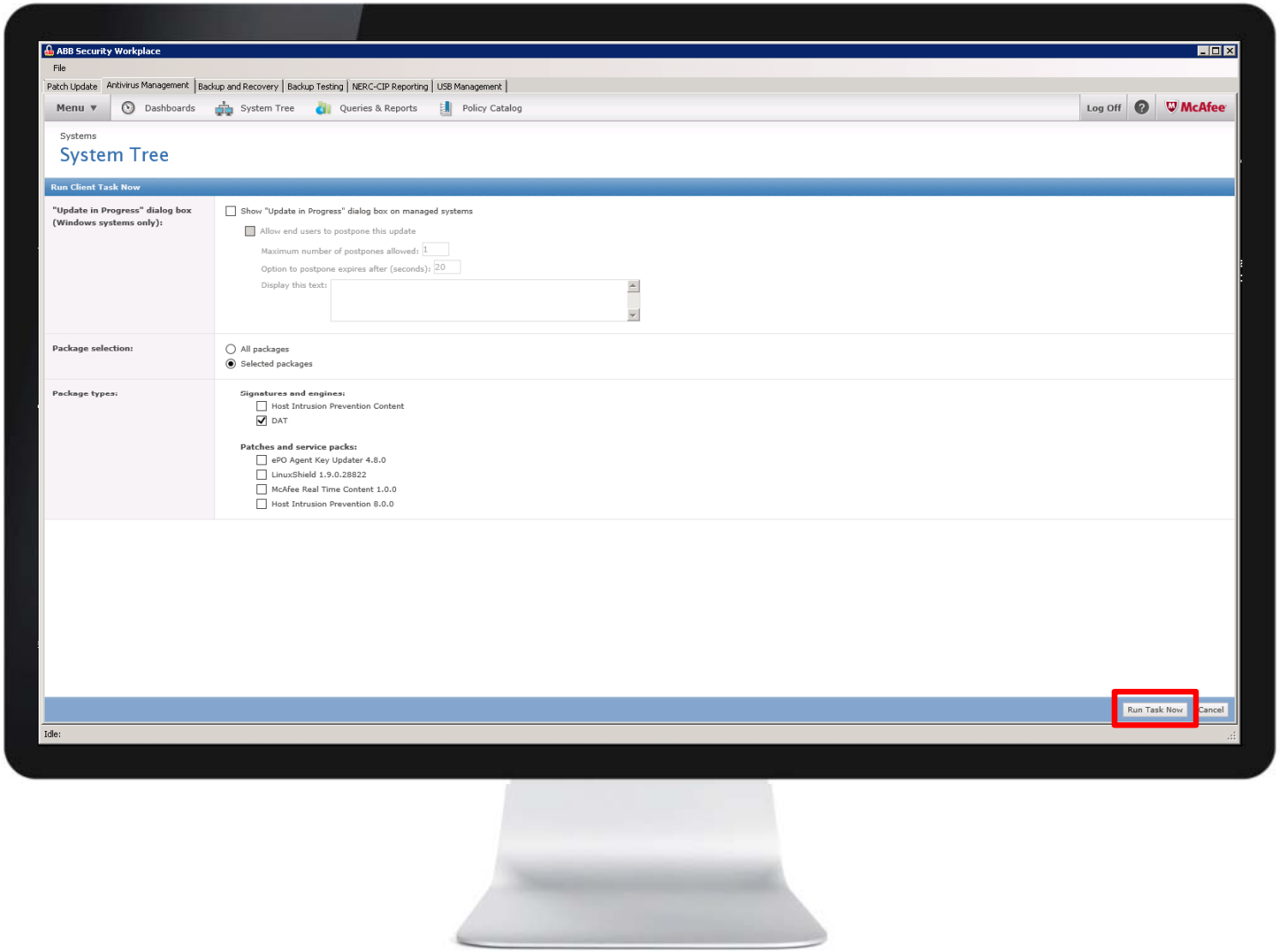


ABB Security Workplace
Maintain - Demonstration

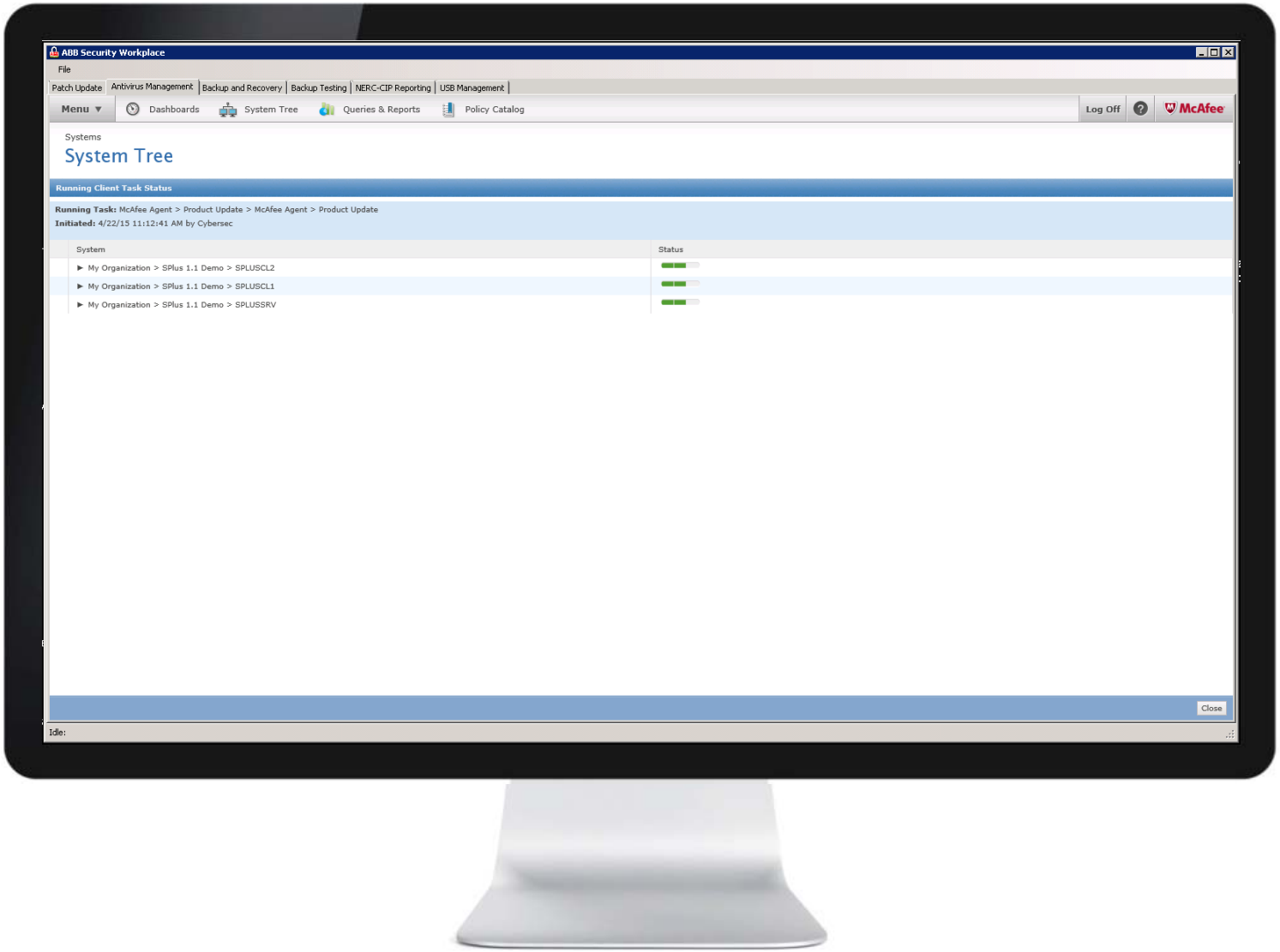
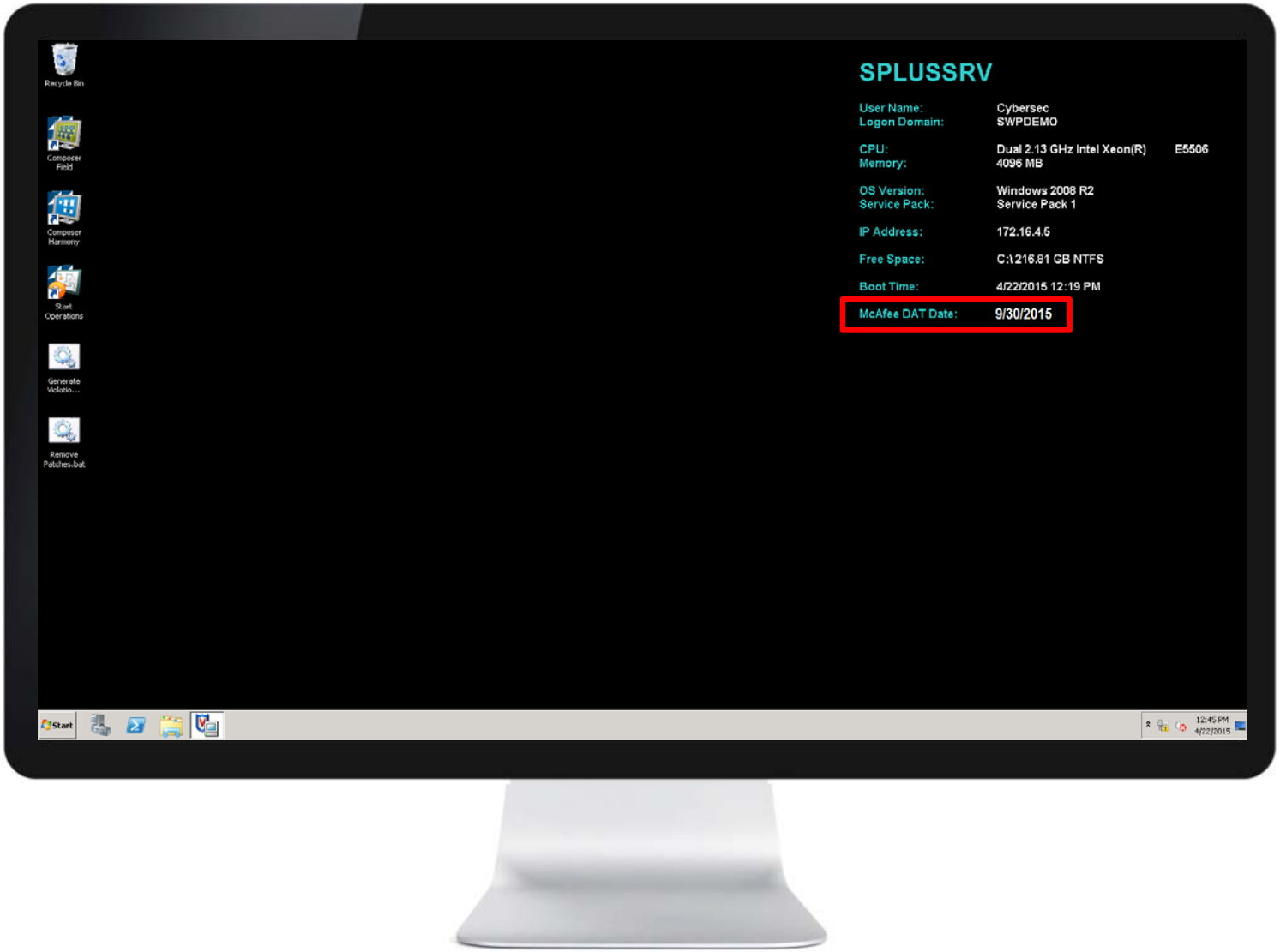


ABB Security Workplace
Maintain - Demonstration



Security Workplace
Package Overview and Maintain Demonstration

Thank You

- Speaker name: Joseph Catanese
- Speaker title: Manager, Cyber Security IAPG
- Phone: 440-585-2789
- E-Mail: joseph.p.catanese@us.abb.com

Power and productivity
for a better world™