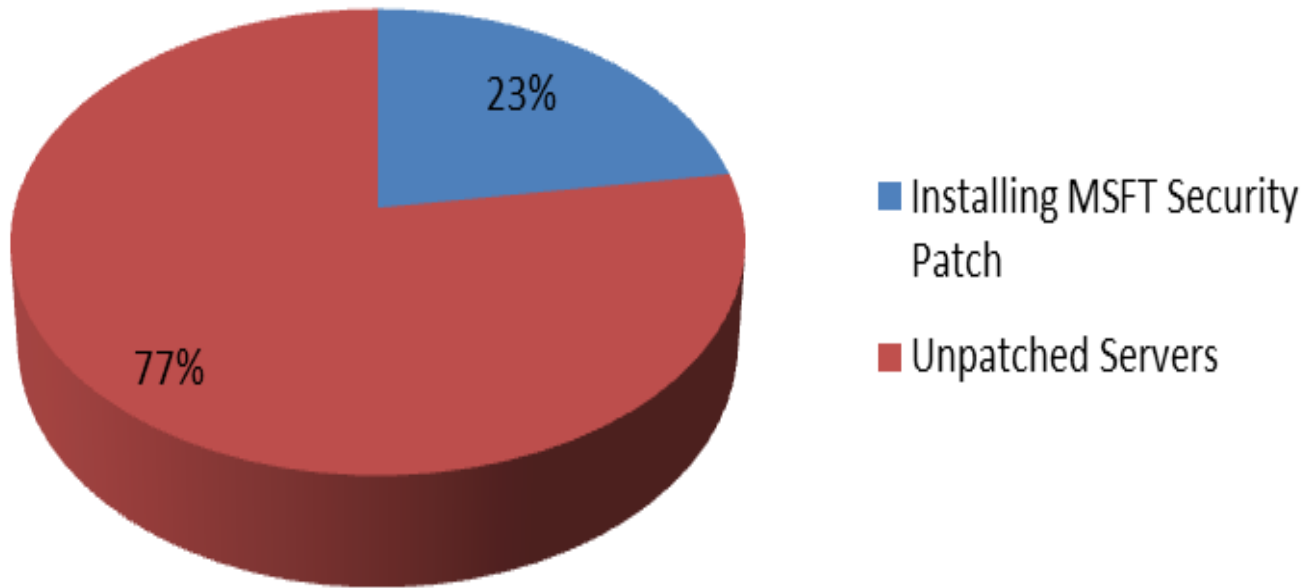


April 23, 2015

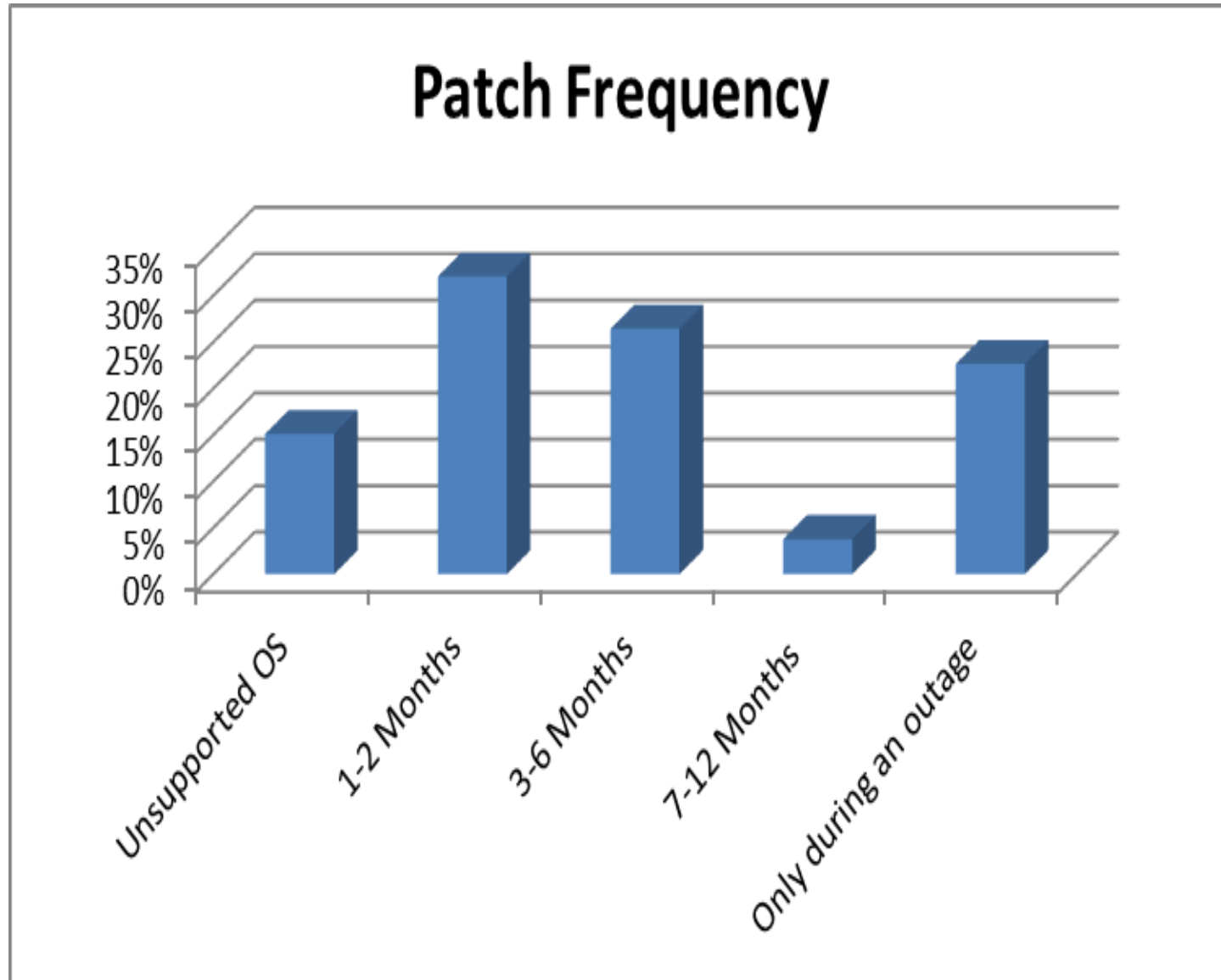
ABB Power Generation DCS Users Group Cyber Security Special Interest Group

Registration Peer Group Survey

Which Poses Greater Threat to Ops?

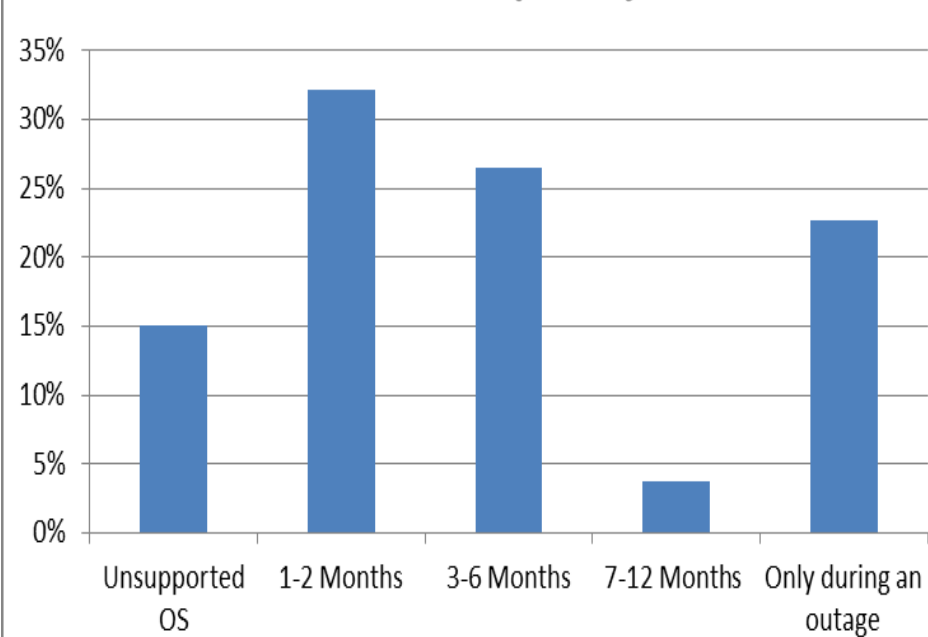


Registration Peer Group Survey

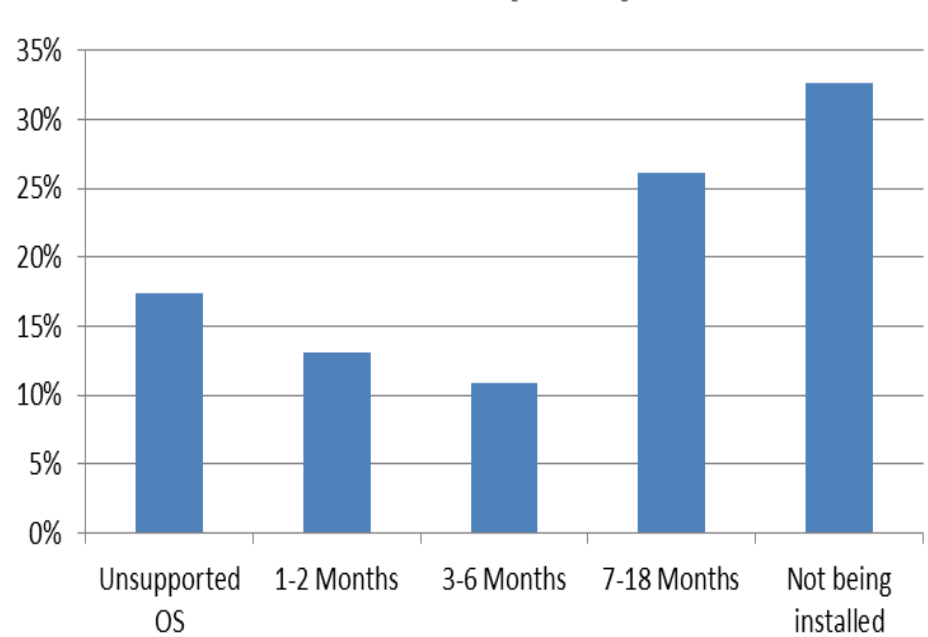


Registration Peer Group Survey

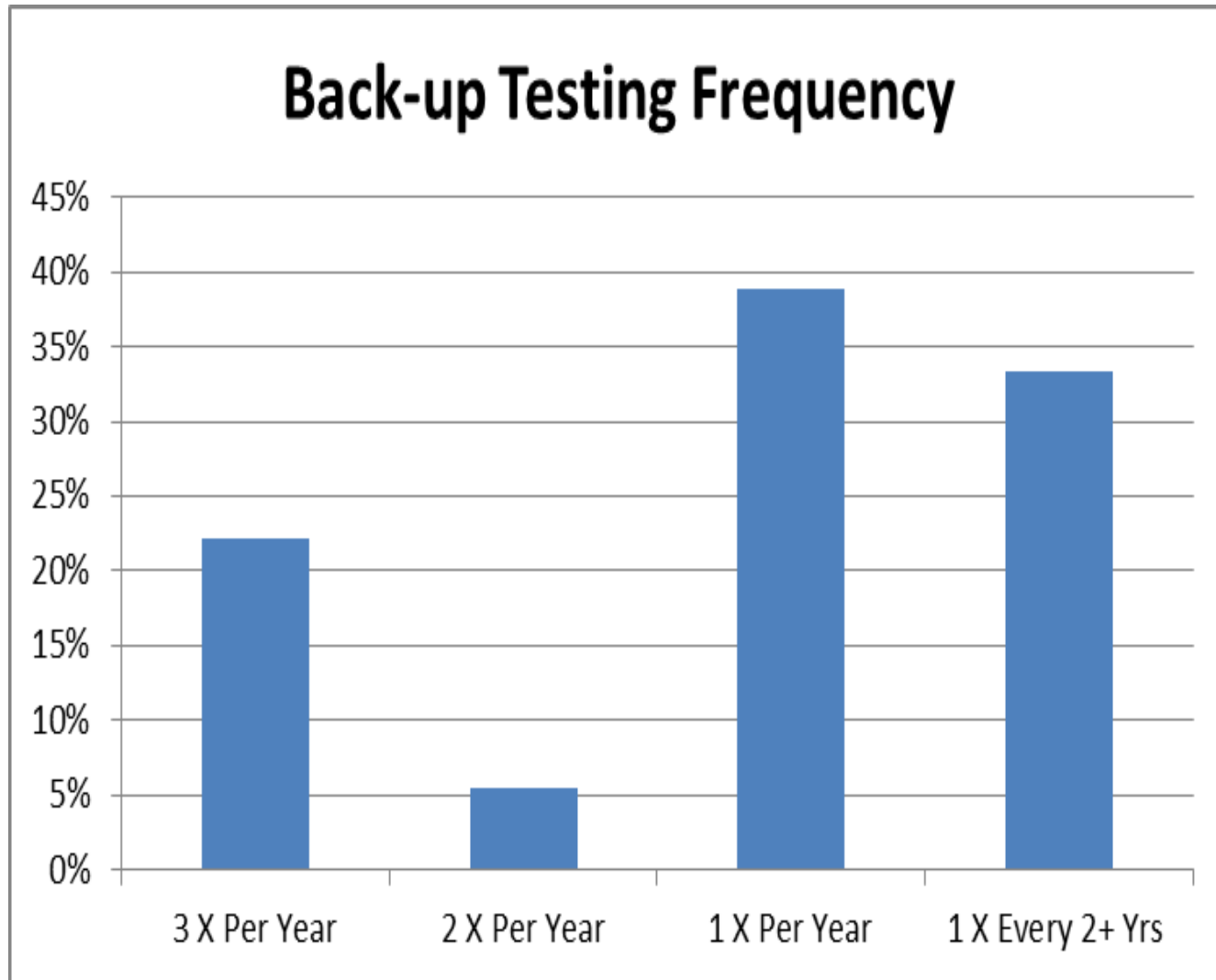
Patch Frequency

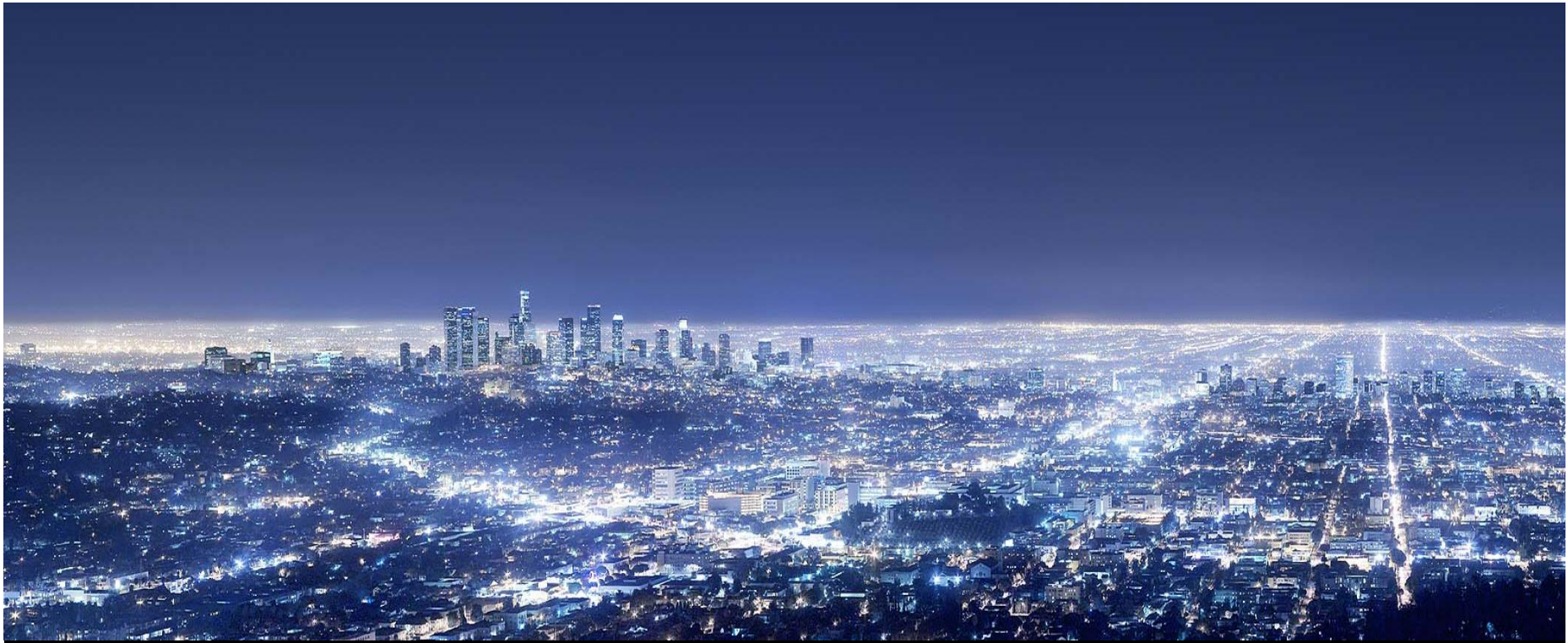


Patch Frequency



Registration Peer Group Survey – Future Topic





April 23, 2015

ABB Power Generation DCS Users Group Cyber Security Special Interest Group ABB Cyber Security Solutions

Join the ABB DCS Users Group

Share, exchange, and connect with your peers!

- **Website:** www.adcsug.com
- Users of ABB control system products and services in the power and water industries.
 - Forum to: share experiences, learn and collaborate with industry peers, measurably influence and improve ABB products and services
- Top 5 reasons to join the group:
 - Networking: true peer-to-peer forums
 - Improvement suggestions: day-to-day challenges discussed and ideas exchanged
 - News: related articles and information from the industry
 - Events calendar: stay connected with users and ABB Power Generation
 - Polls / surveys: express your opinion and make your voice heard
- “The value of a users group, and that in particular of ABB DCS Users Group, is that as a group we have more access and leverage to change and improve the product than as individuals acting alone. It also allows us to participate in discussions that bring the best ideas forward and facilitates sharing information that helps everyone.” - Bill Ossman, ABB DCS Users Group STECO member



ABB Power Generation Cyber Security Special Interest Group

Agenda

- Welcome & Introductions
- ABB Security Solutions Overview
- MAINTAIN Demonstrations
- Response Polling
- Conclude
- Pop-Up Response Survey (5-minutes of your time)

Today's Panel

- Mike Radigan, Senior Advisor, Cyber Risk Management, ABB PSPG
 - Mike.Radigan@us.abb.com (614) 398-6241
- Joe Catanese, Application Engineer, ABB Power Generation
 - joseph.p.catanese@us.abb.com (440) 585-2789
- Matt Virostek, Application Engineer, ABB Power Generation
 - matthew.virostek@us.abb.com (440) 585-2789

ABB Power Generation Cyber Security Special Interest Group

Agenda

- Welcome & Introductions
- **ABB Security Solutions Overview**
- MAINTAIN Demonstrations
- Response Polling
- Conclude
- Pop-Up Response Survey (5-minutes of your time)

Security Workplace

Package Overview and Maintain Demonstration



- Speaker name: Joe Catanese
- Speaker title: Sr. Application Engineer – Cyber Security
- Company name: ABB Inc.
- Location: Wickliffe, Ohio
- Phone: 440-585-2789
- E-Mail: joseph.p.Catanese@us.abb.com

Presentation Outline Overview

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

Security Workplace Package Overview

Security Workplace Package overview



MAINTAIN

Security Workplace

- System Hardening
- User Access Control
- MS Patches, Anti Virus, Patch Disk
- **Centralized Microsoft Patching***
- Centralized Anti-Virus Management
- Automated Backup and Recovery
- **Secure File Transfer (ODI-X)***

DEFEND

- **Detect-in-Depth (Sophia)***
- NIDS (Network Intrusion Detection)
- Security Event Monitoring
- **Application Whitelisting ***
- Configuration Change Management
- IT Asset Management

COMPLY

- Automated Data Collection
- Automated Compliance Reporting
- Workflow Automation Suite

Security Workplace Package overview

Security Baseline Requirements**	MAINTAIN	DEFEND	COMPLY
Automated back-up & recovery	✓	✓	✓
System and network hardening	✓	✓	✓
Centralized anti-virus management	✓	✓	✓
Centralized Microsoft patch management	✓	✓	✓

Proactive Security Measures

Electronic perimeter protection*		✓	✓
Security event management*		✓	✓
ICS asset management*		✓	✓
Configuration change management*		✓	✓
Automated data collection*		✓	✓

NERC CIP Compliance

Automated compliance reporting*		✓
Policy management*		✓
Workflow Automation Suite		✓

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

**Active ServiceGrid contract required

✓ = Included

ABB Security Workplace

NERC-CIP version 5 Requirements

002 BES Cyber System Categorization	003 Security Management Controls	004 Personnel and Training	005 Electronic Security Perimeter	006 Physical Security of CCAs	007 System Security Management	008 Incident Reporting and Response Planning	009 Recovery Plans for CCAs	010 Change Management and Vulnerability Assessments	011 Information Protection
Impact Rating	Cyber Security Policy	Awareness	Electronic Security Perimeter	Physical Security Plan	Test Procedures	Incident Response Plan	Recovery Plan	Configuration Change Management	Information Protection
15 Month Review	Management Approval	Cyber Security Training	Remote Access Management	Visitor Control Program	Ports and Services	Implementation and Testing	Exercises	Configuration Monitoring	Media Reuse and Disposal
	Leadership	Personnel Risk Assessment		PACS Maintenance and Testing	Security Patch Management	Review, Update and Communicate	Change Control	Vulnerability Assessment	
	Delegation	Access Management Plan		Physical Access Controls	Malicious Software Prevention				
		Access Revocation			Security Event Monitoring				
					System Access Controls				

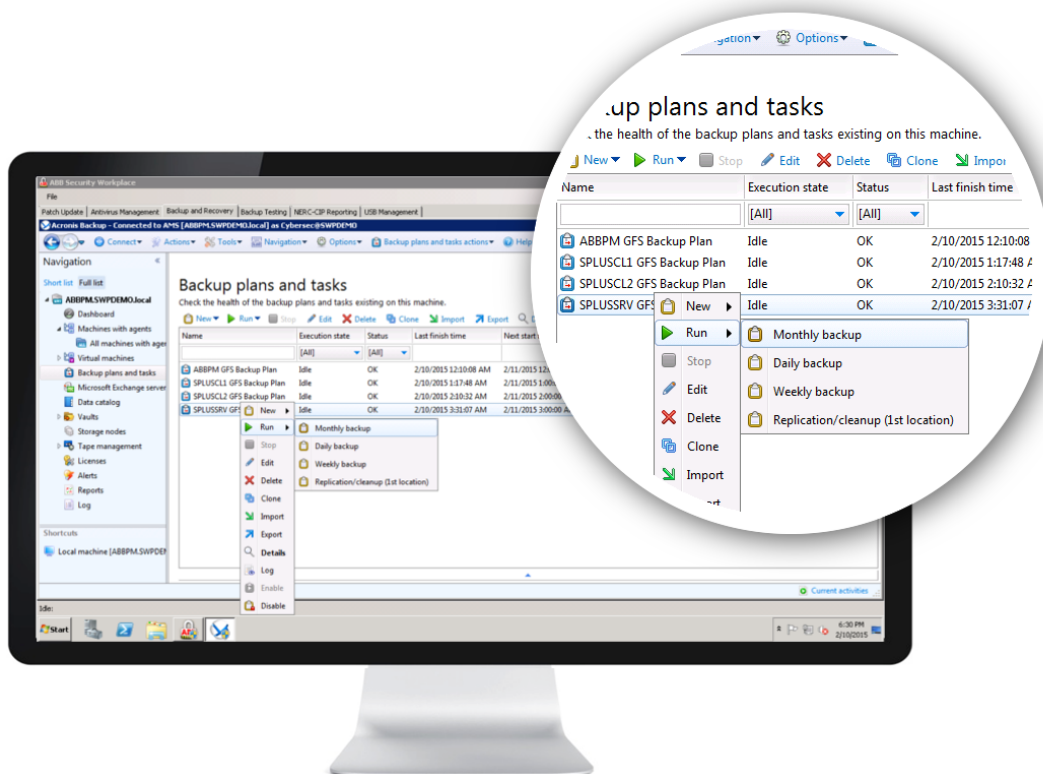
•Security Workplace assists in compliance of requirements marked by



Security Workplace

Maintain Package

ABB Security Workplace Maintain



- Grandfather – Father – Son
- Centrally manages backup plans
- Recovery plans
- Conversion to VM

ABB Security Workplace Maintain



Automated
Backup & Recovery

System &
Network Hardening



Centralized Anti-
Virus Management



Centralized Microsoft
Patch Management

- Reduce surface area of vulnerability
 - Services
 - Firewall
 - Applications
- Close unused networking ports
- System state documentation

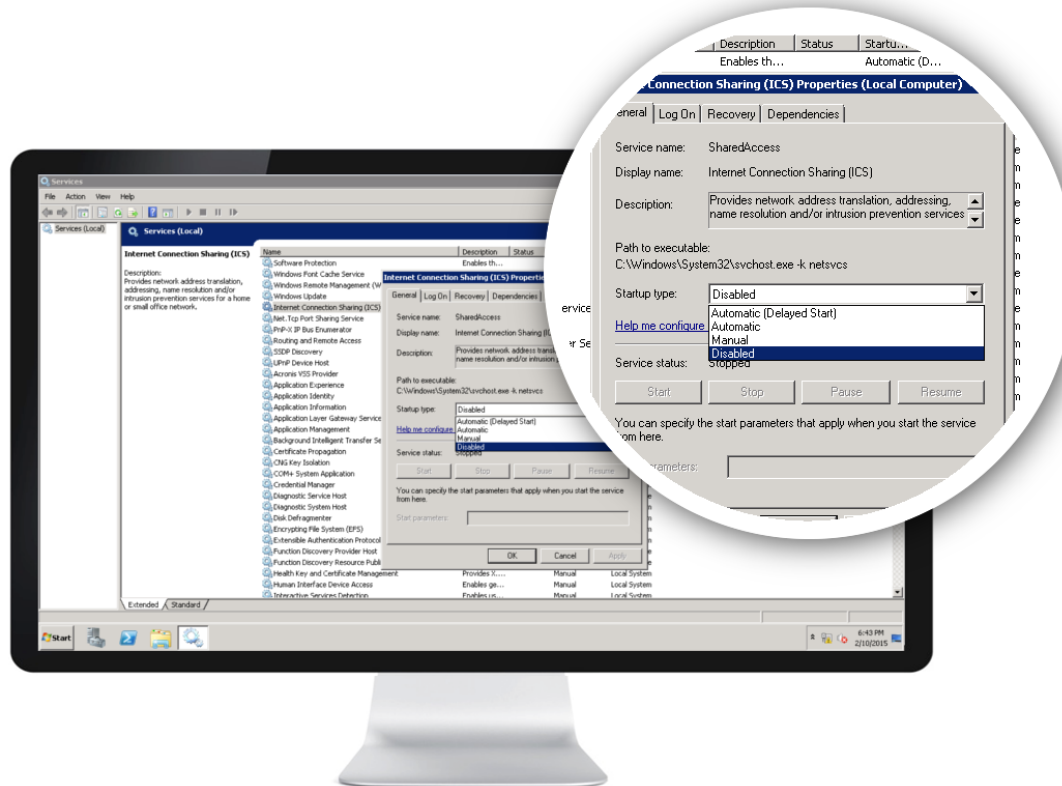


ABB Security Workplace Maintain



Automated
Backup & Recovery



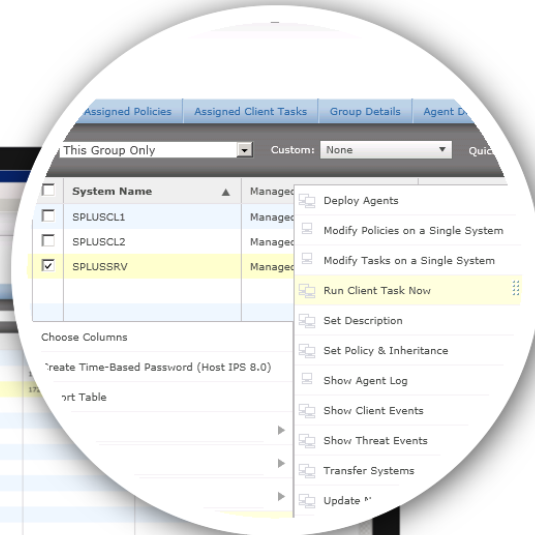
System &
Network Hardening



Centralized Anti-
Virus Management



Centralized Microsoft
Patch Management



- Manage AV Policies
- Manage DAT file deployments

ABB Security Workplace Maintain



Automated
Backup & Recovery



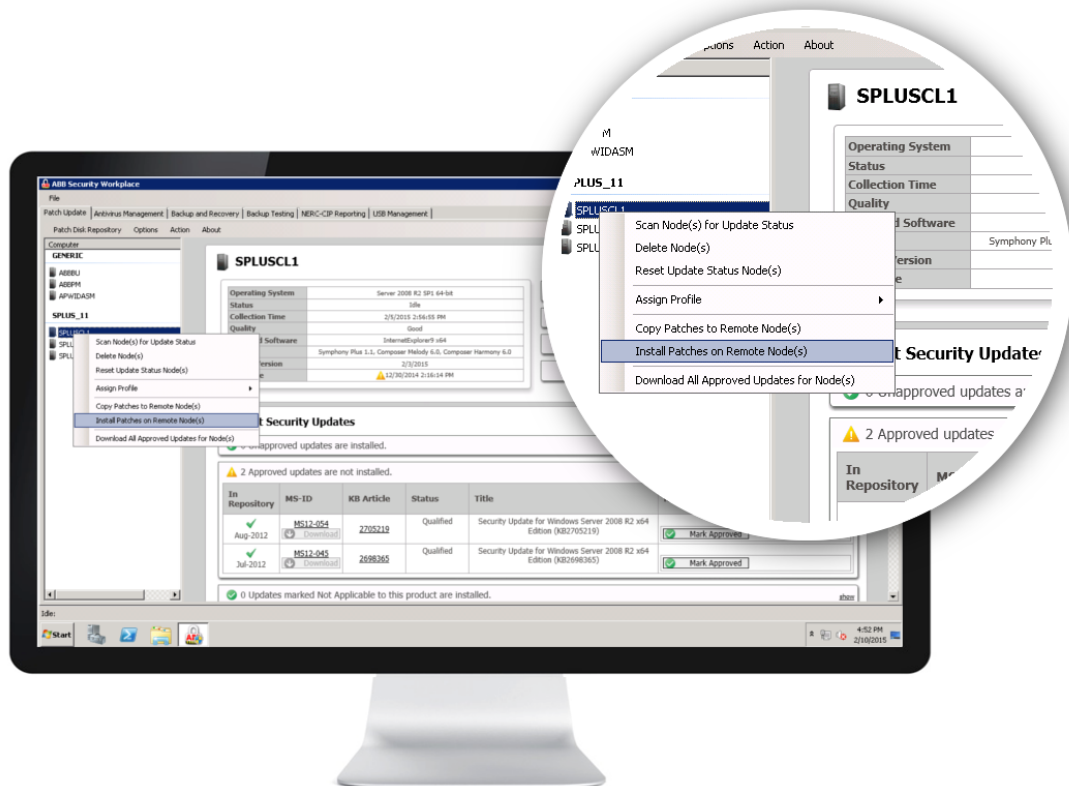
System &
Network Hardening



Centralized Anti-
Virus Management



Centralized Microsoft
Patch Management



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

Security Workplace

Defend Package

ABB Security Workplace Defend

**Electronic
Perimeter Protection**

**Security
Event Management**

**ICS Asset
Management**

**Configuration Change
Management**

- Edge Routing/Firewall
- Intrusion Protection
- Unified Threat Manager
- IPSec / SSL VPN

ABB Security Workplace Defend



Electronic
Perimeter Protection



Security
Event Management



ICS Asset
Management



Configuration Change
Management



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

ABB Security Workplace Defend



Electronic
Perimeter Protection



Security
Event Management



ICS Asset
Management



Configuration Change
Management



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

ABB Security Workplace Defend



Electronic
Perimeter Protection



Security
Event Management



ICS Asset
Management



Configuration Change
Management



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

Security Workplace Comply Package

Automated Compliance Reporting

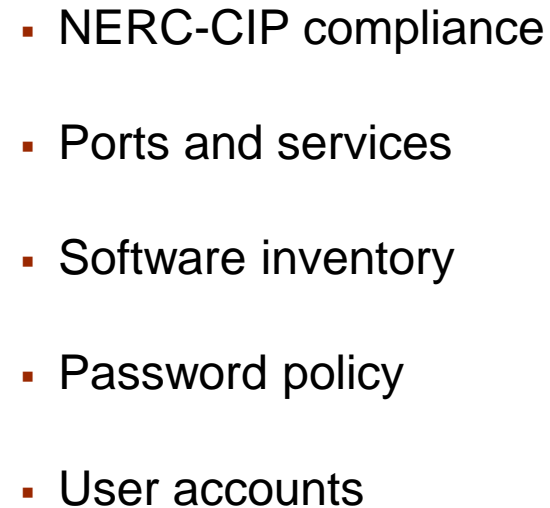


ABB Security Workplace Comply



Automated Compliance
Reporting



Policy
Management



Workflow
Automation Suite



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

ABB Security Workplace Comply



Automated Compliance
Reporting



Policy
Management



Workflow
Automation Suite



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

Security Workplace

Continuing Development

ABB Security Workplace Continuing development

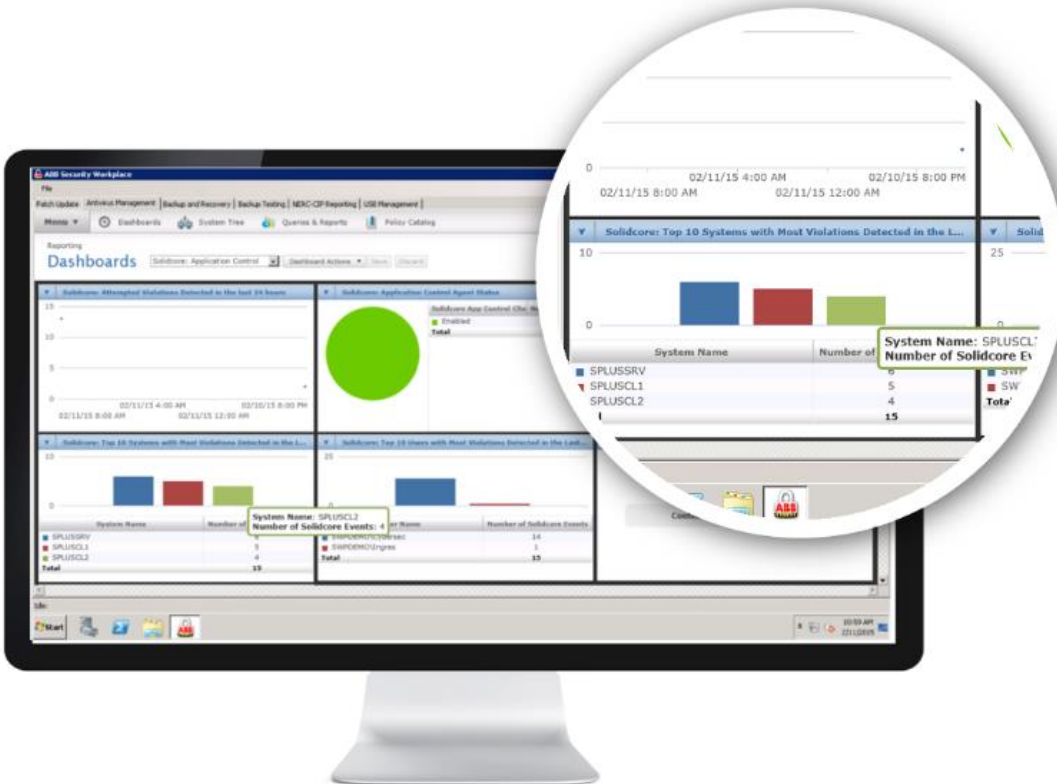
Application
Control



USB/Media
Control



Disaster
Recovery



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

ABB Security Workplace

Continuing development



Application
Control

USB/Media
Control



Disaster
Recovery

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

Indexed files log of Odix Stations

Show 15 entries

ID	Timestamp	Station name	Username	Scan code
14173	2015-02-10 17:20:31	abb-demo	Cybersec	611f3e2cb651
14172	2015-02-10 17:20:31	abb-demo	Cybersec	611f3e2cb651
14171	2015-02-10 17:20:31	abb-demo	Cybersec	611f3e2cb651
14170	2015-02-10 17:20:31	abb-demo	Cybersec	611f3e2cb651
14169	2015-02-10 17:20:31	abb-demo	Cybersec	611f3e2cb651
14168	2015-02-10 17:20:31	abb-demo	Cybersec	611f3e2cb651
14167	2015-02-10 17:20:31	abb-demo	Cybersec	611f3e2cb651
14166	2015-02-10 17:20:31	abb-demo	Cybersec	611f3e2cb651
14165	2015-02-10 17:20:31	abb-demo	Cybersec	611f3e2cb651

ABB Security Workplace Continuing development



Application
Control



USB/Media
Control



Disaster
Recovery

- Alternative to Acronis
- Dell OEM driver support
- Tighter integration with SWP
- Easier to manage



Security Workplace

Maintain Package Walkthrough

ABB Security Workplace Maintain - Demonstration

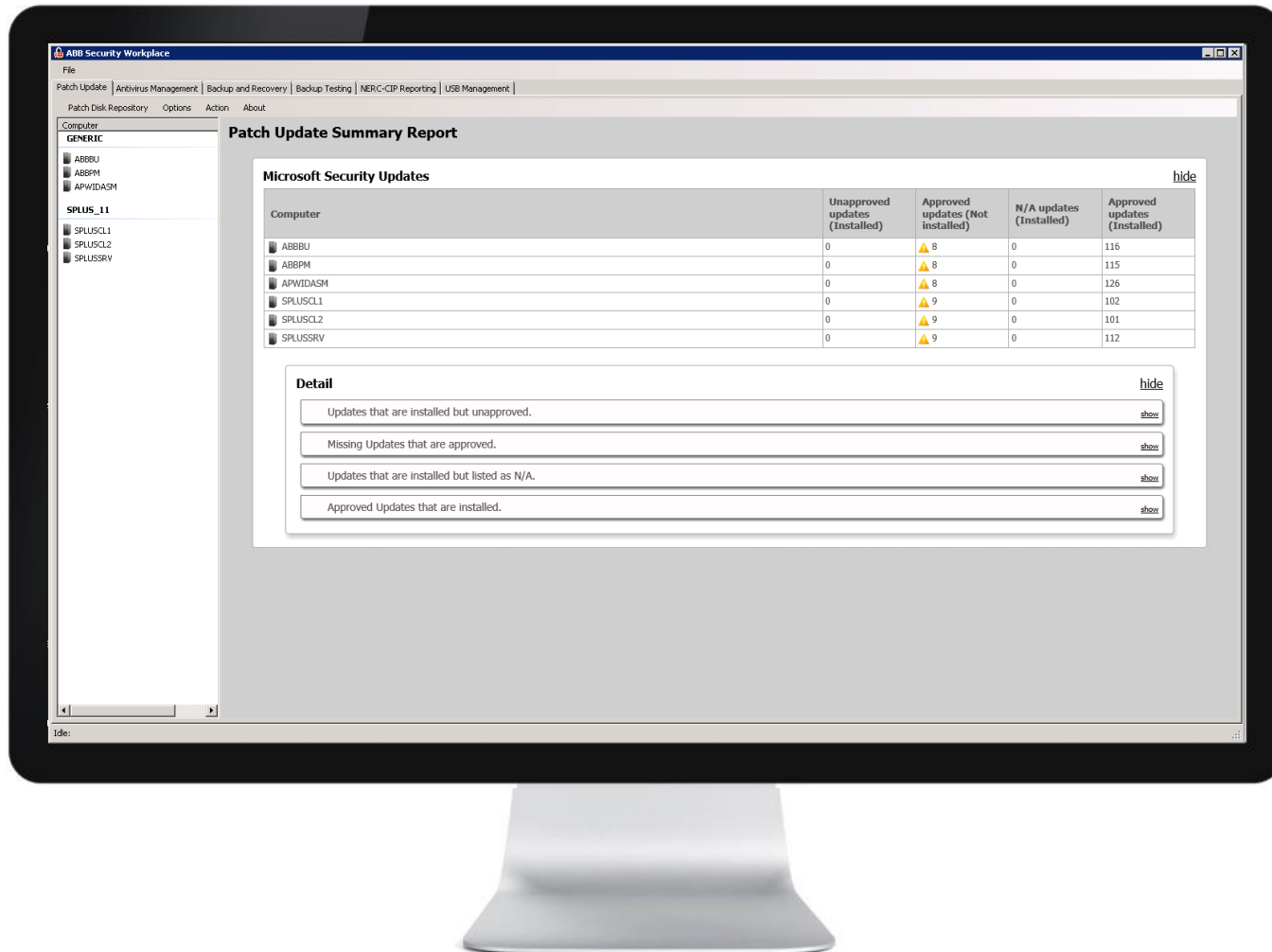


ABB Security Workplace Maintain - Demonstration

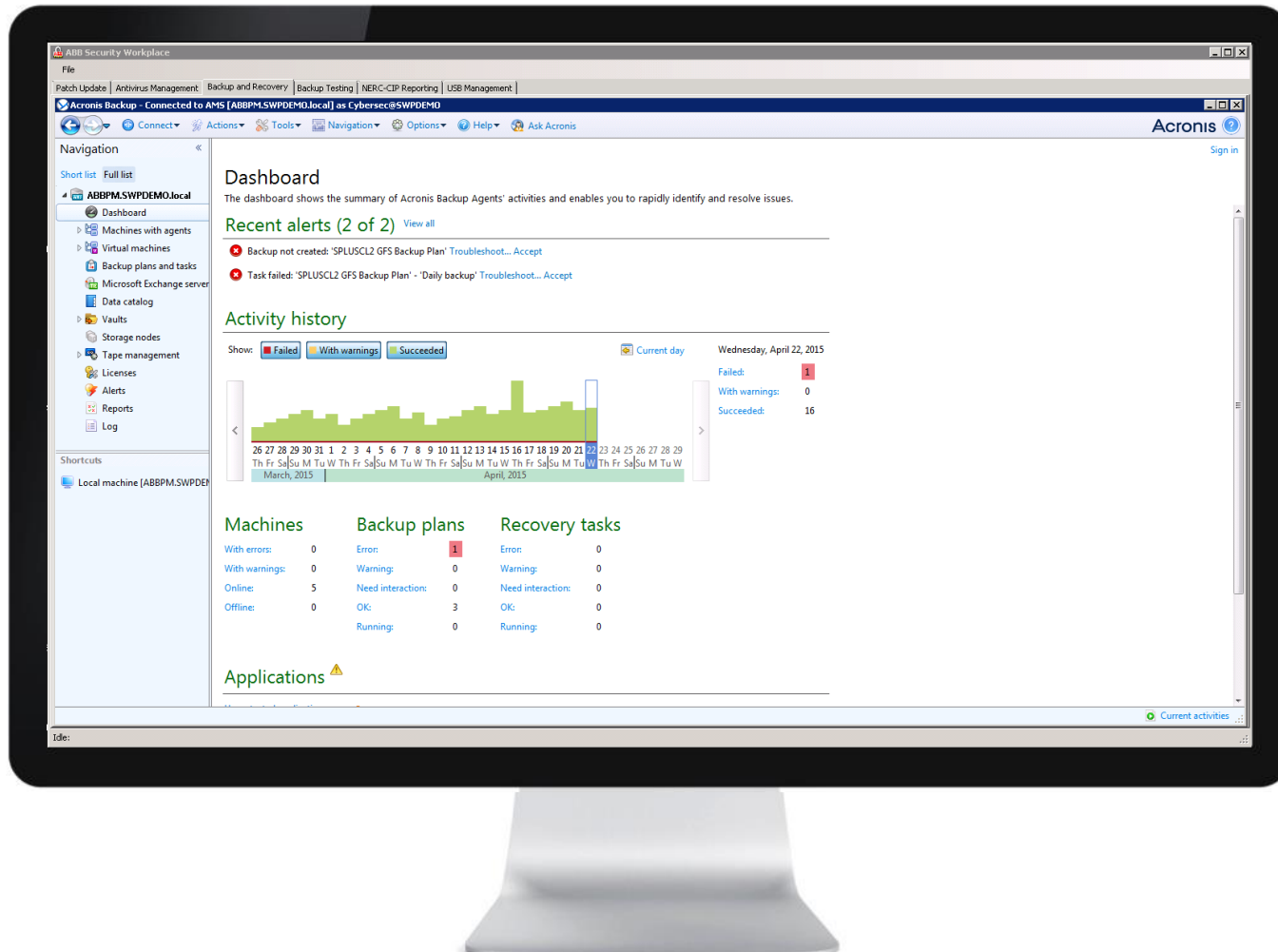




ABB Security Workplace Maintain - Demonstration

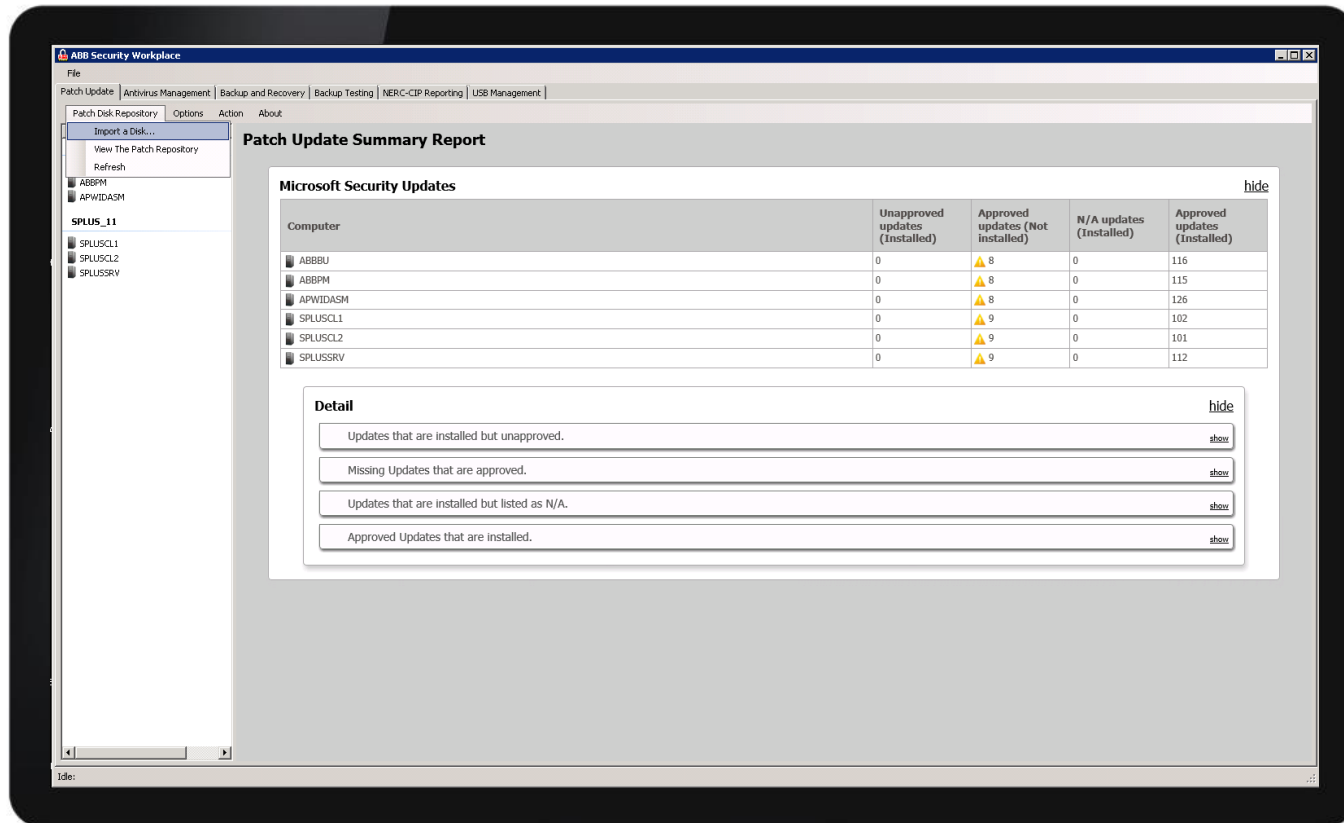


ABB Security Workplace Maintain - Demonstration

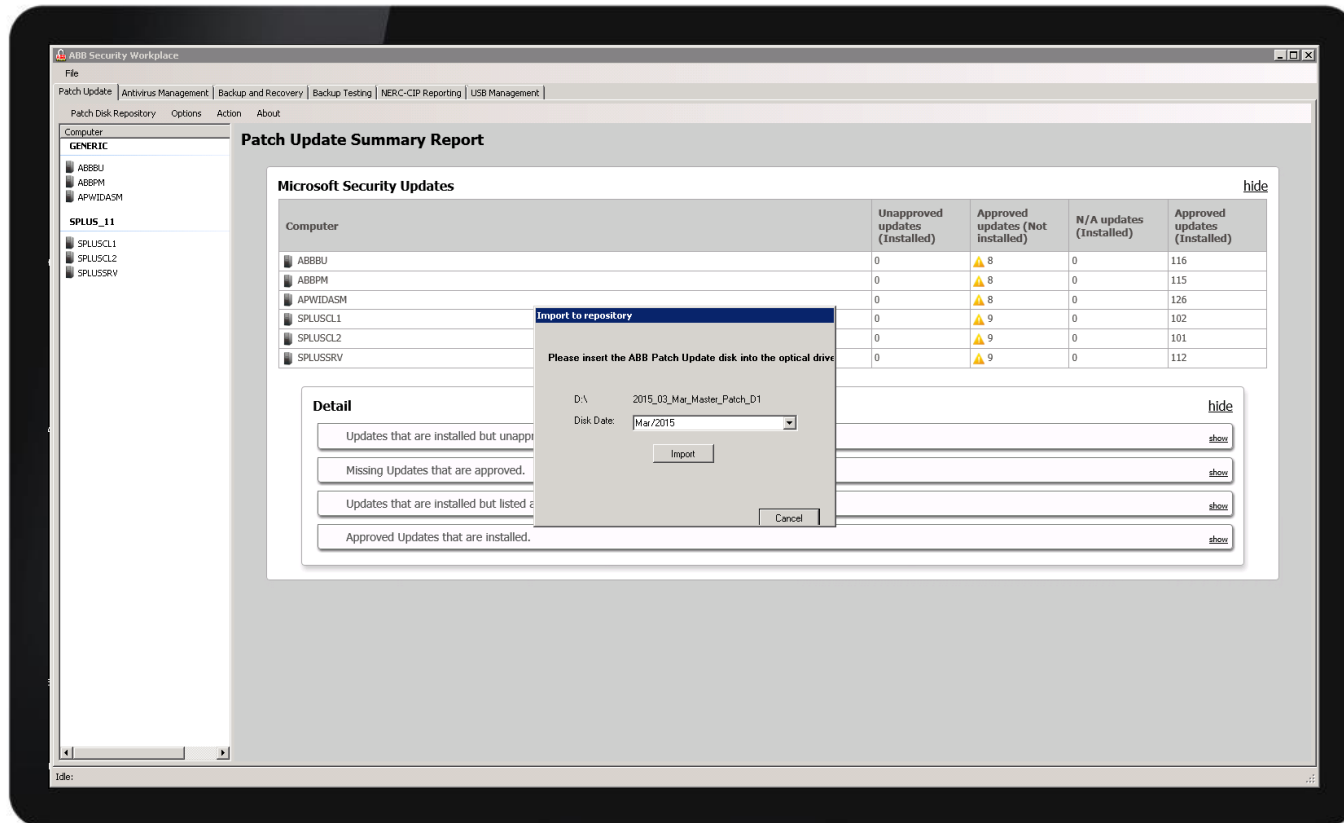


ABB Security Workplace Maintain - Demonstration

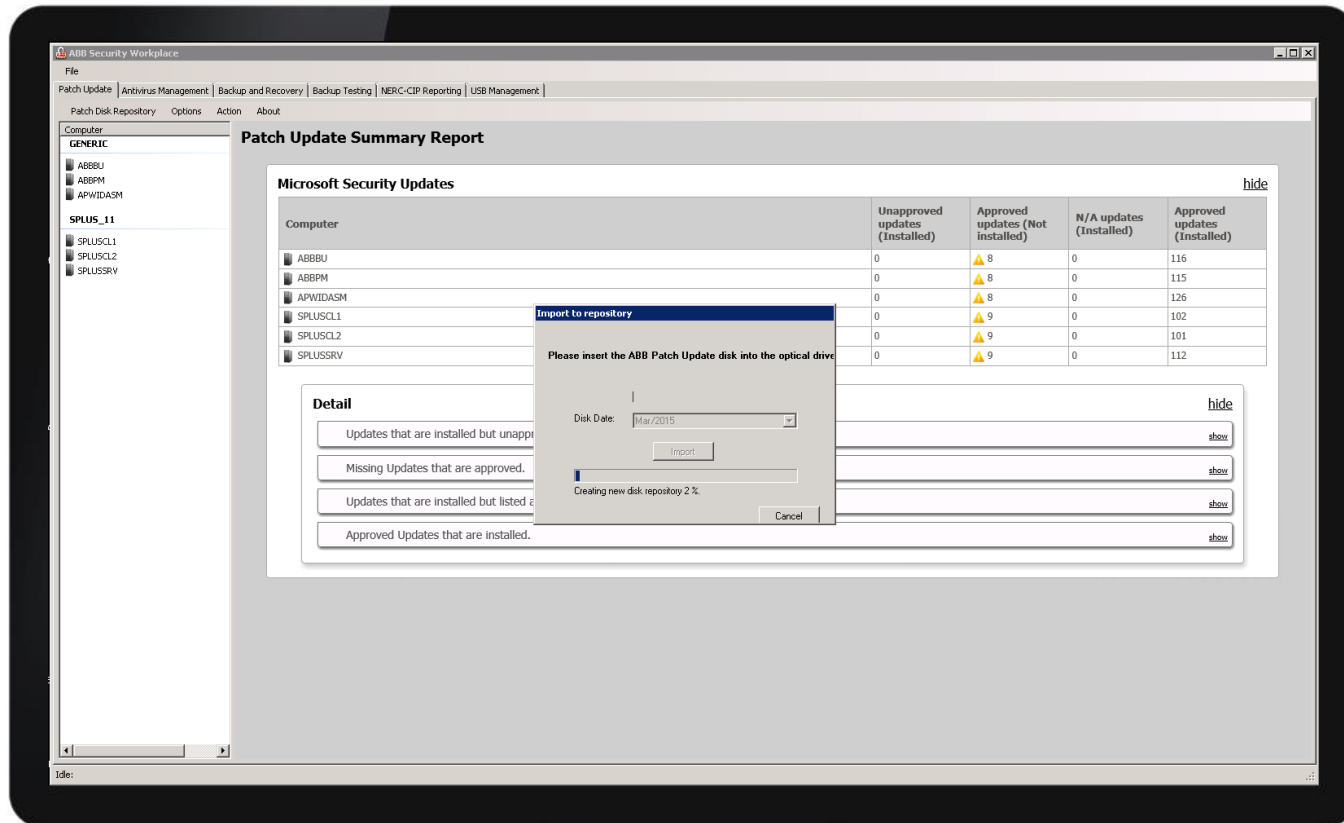


ABB Security Workplace Maintain - Demonstration

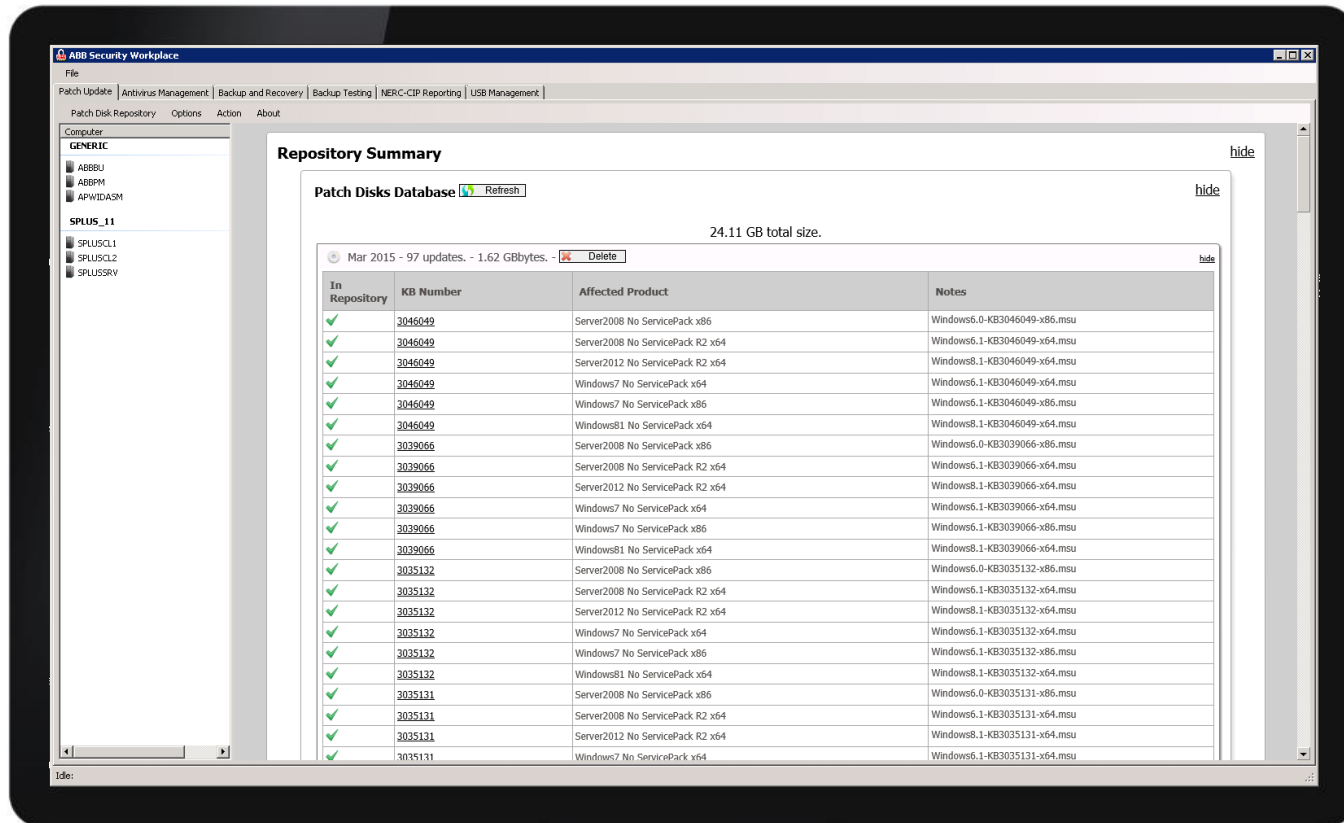


ABB Security Workplace Maintain - Demonstration

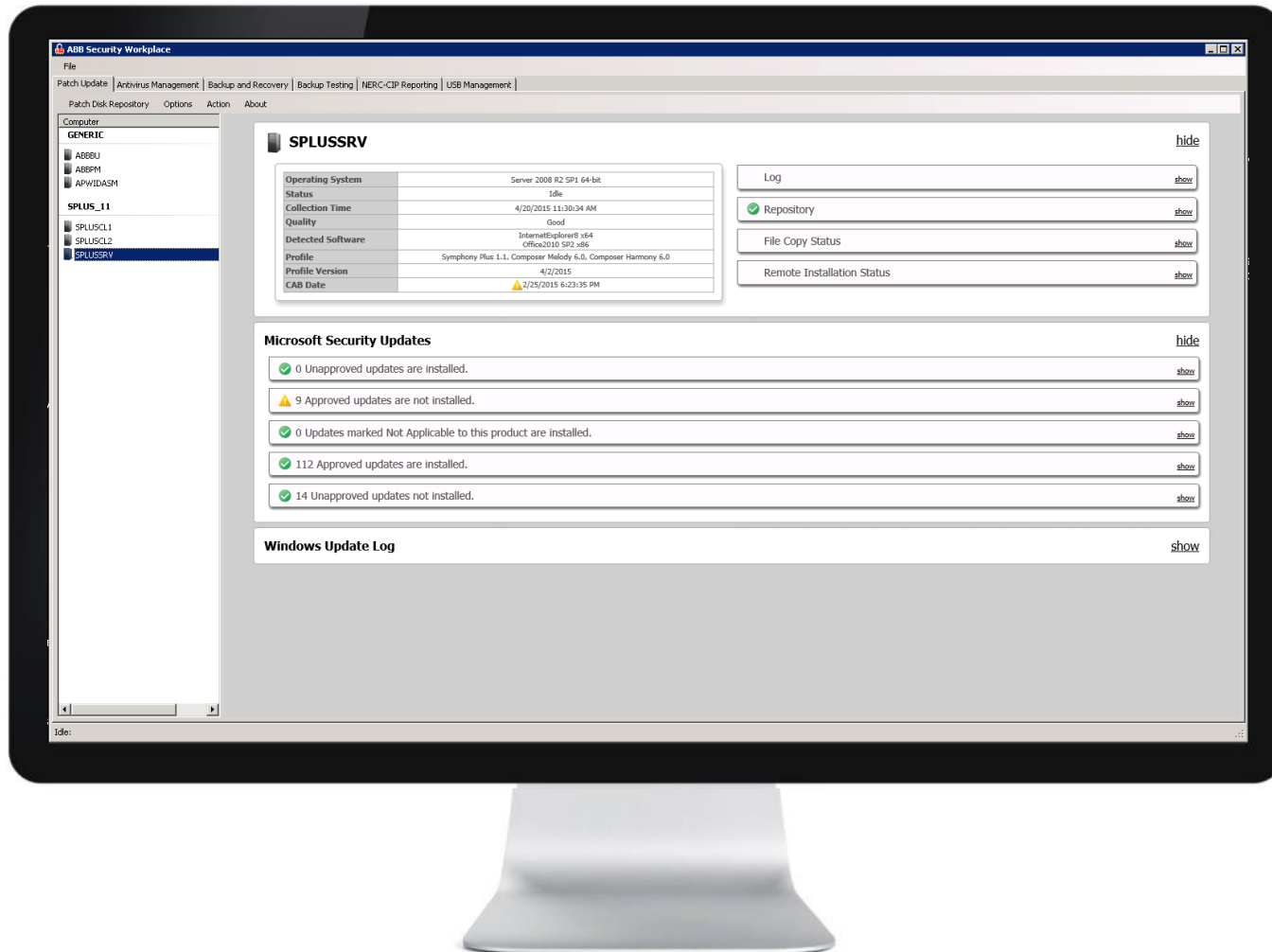


ABB Security Workplace Maintain - Demonstration

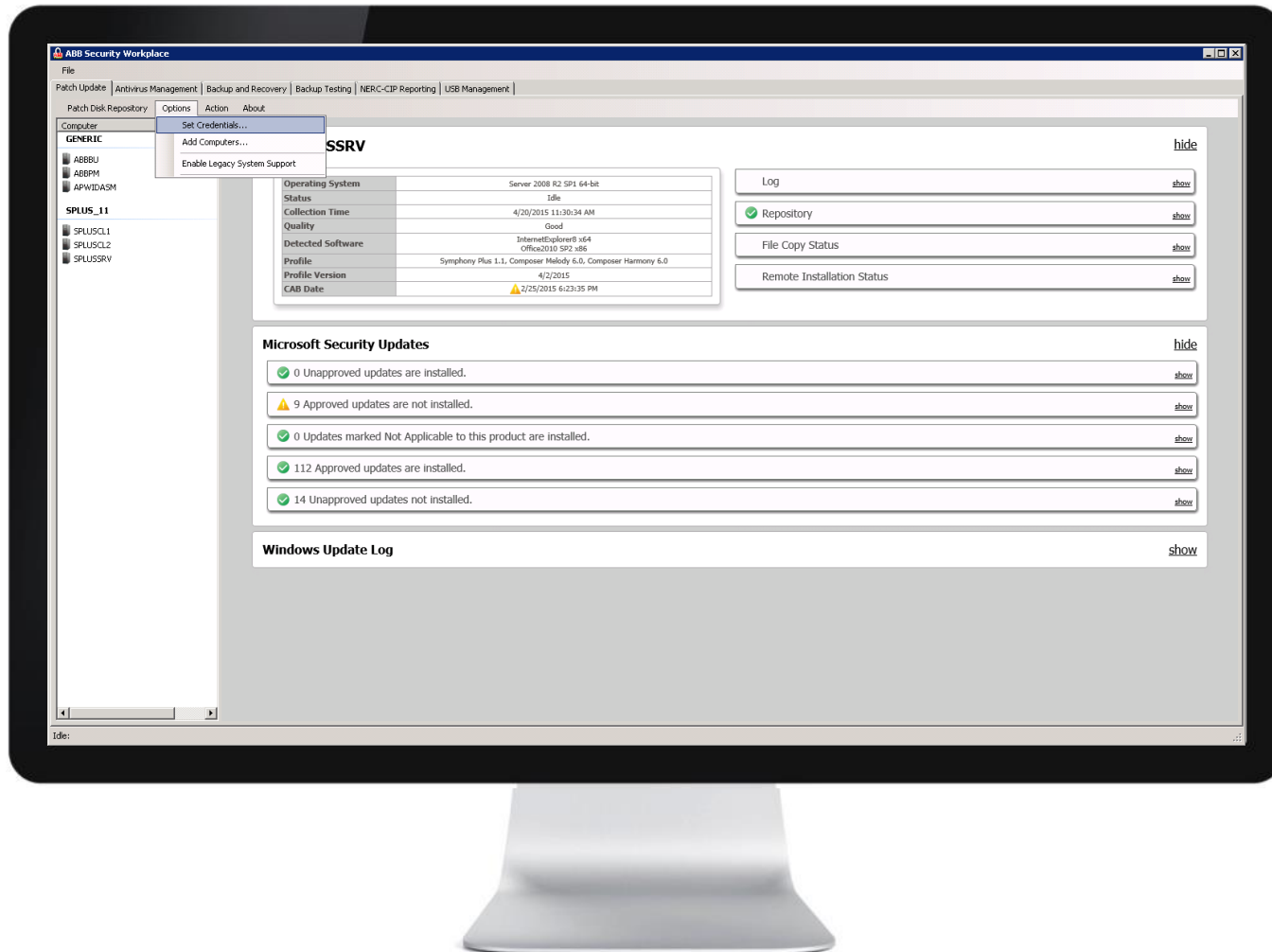


ABB Security Workplace Maintain - Demonstration

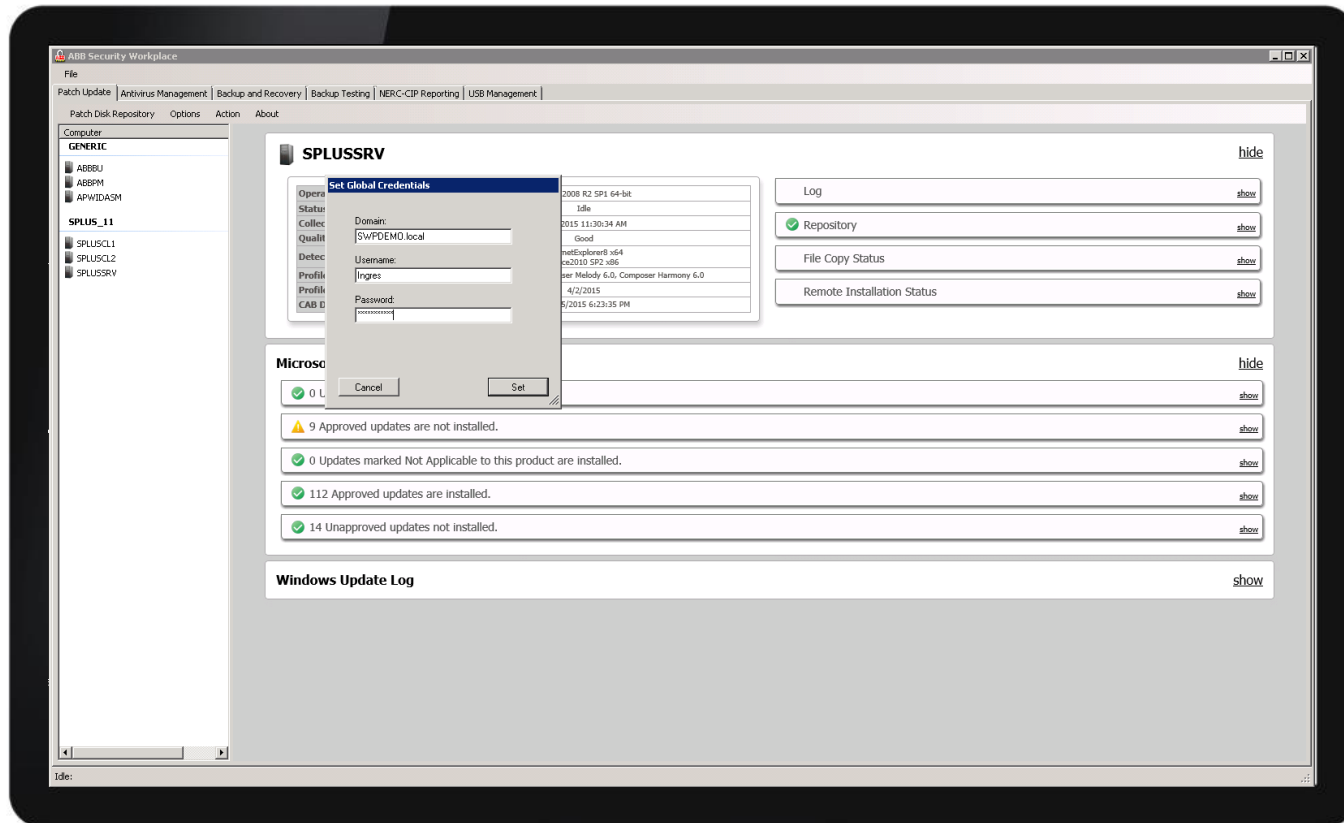


ABB Security Workplace Maintain - Demonstration

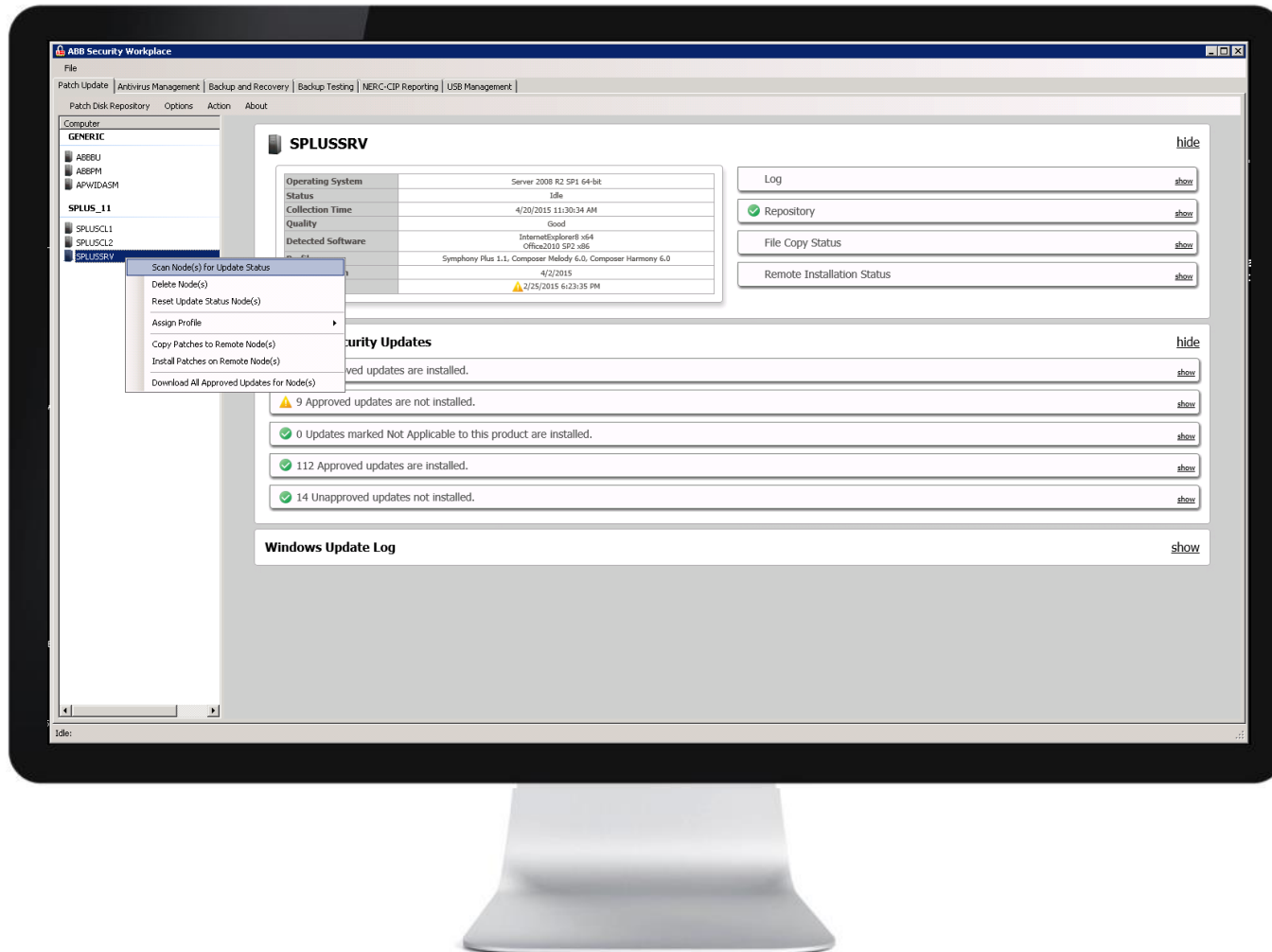


ABB Security Workplace Maintain - Demonstration

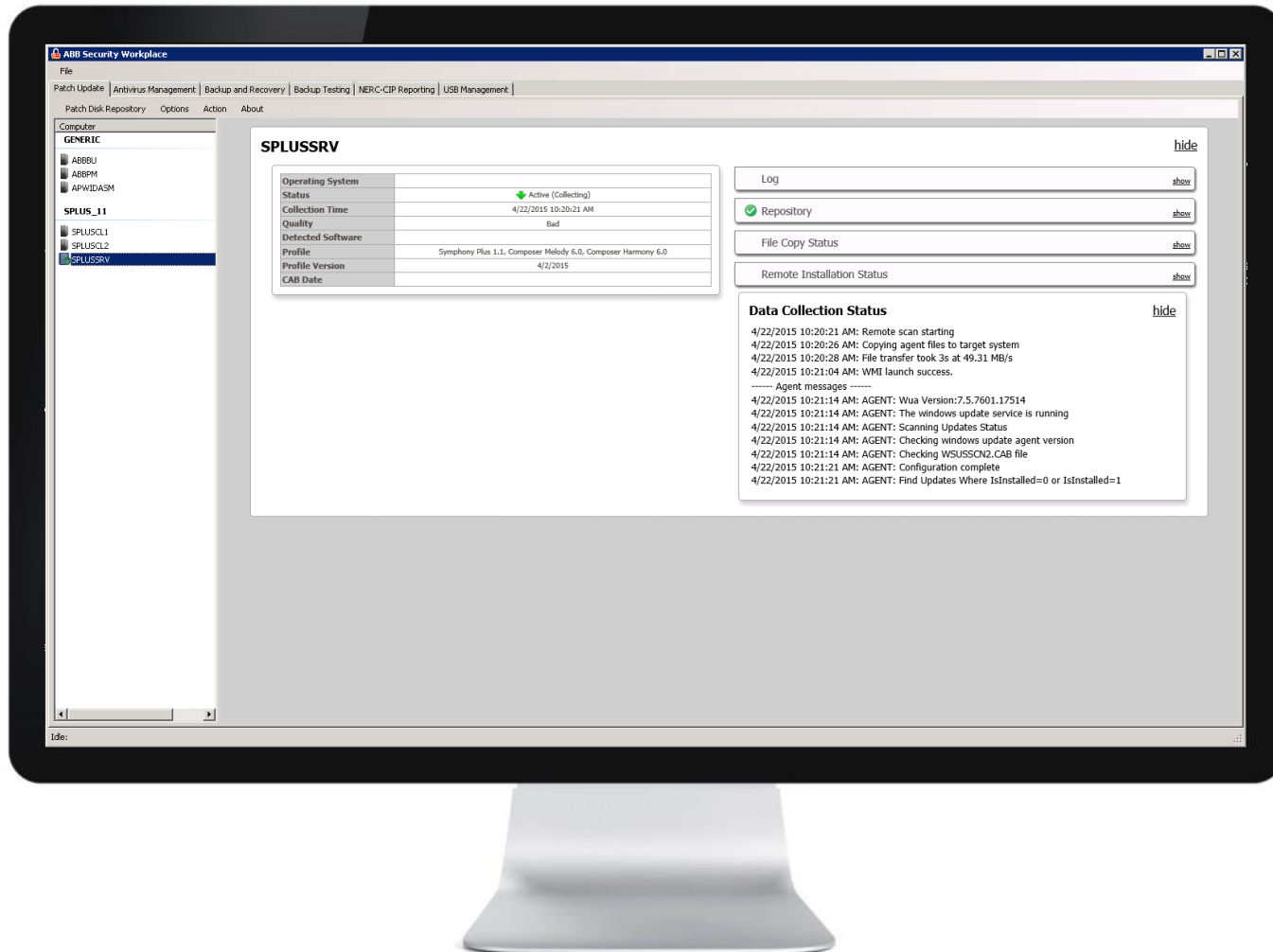


ABB Security Workplace Maintain - Demonstration

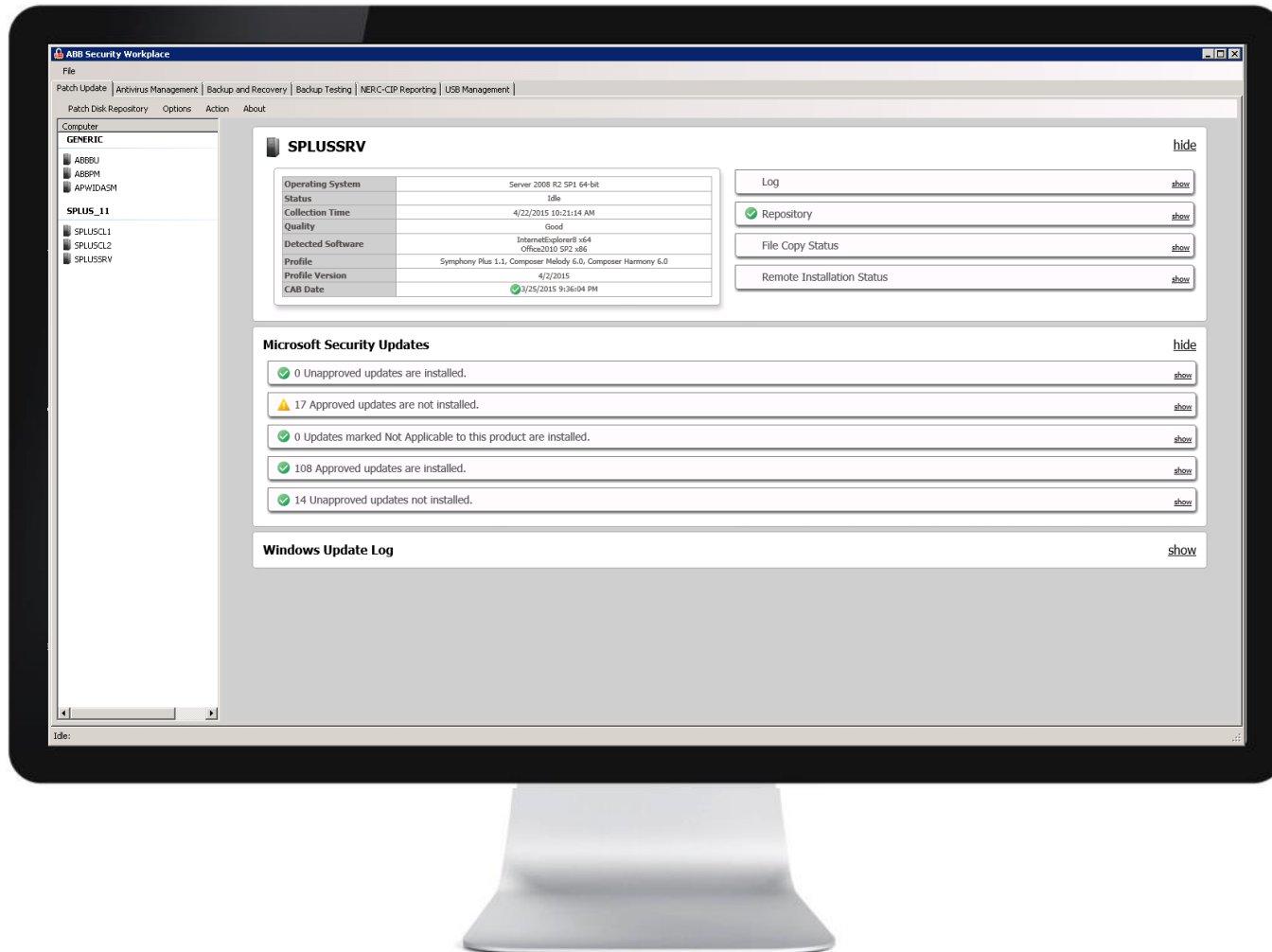


ABB Security Workplace Maintain - Demonstration

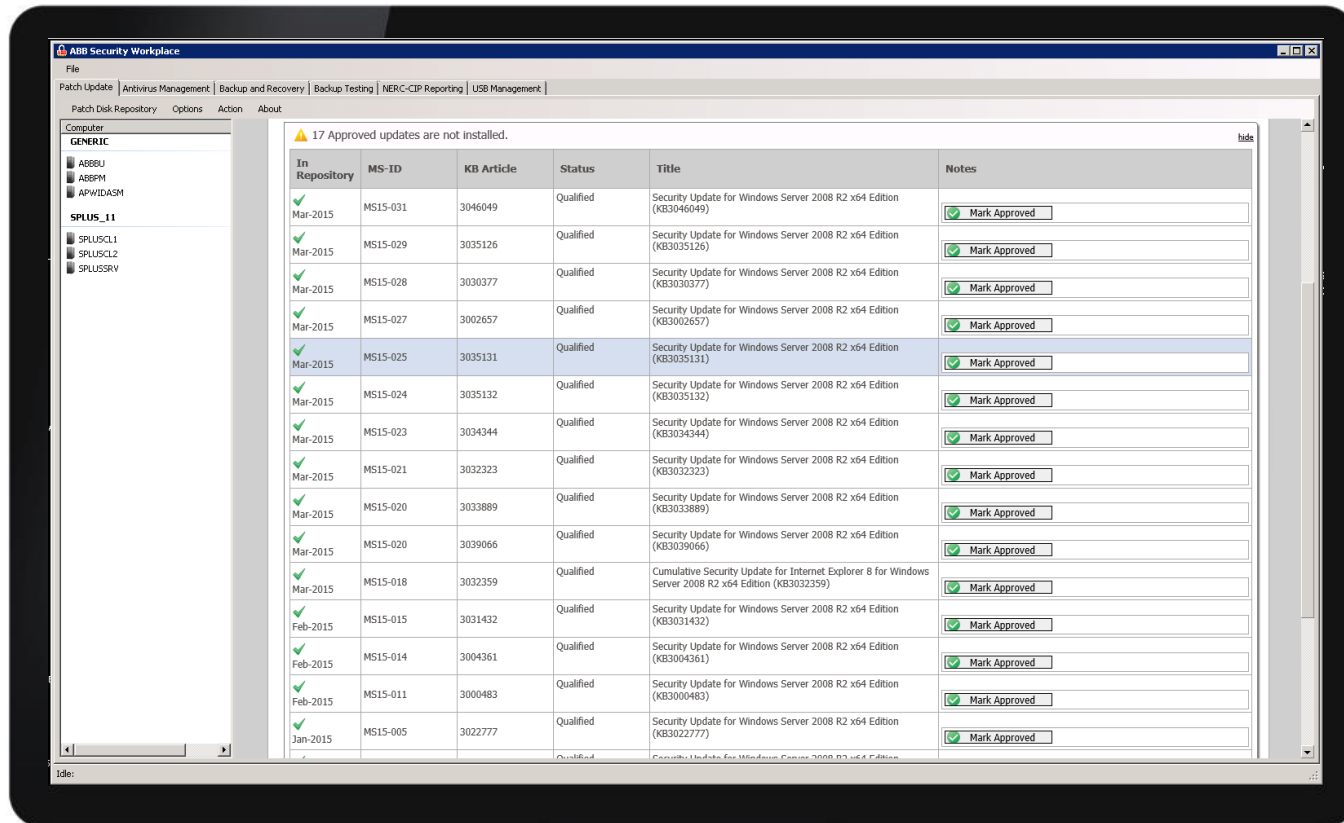


ABB Security Workplace Maintain - Demonstration

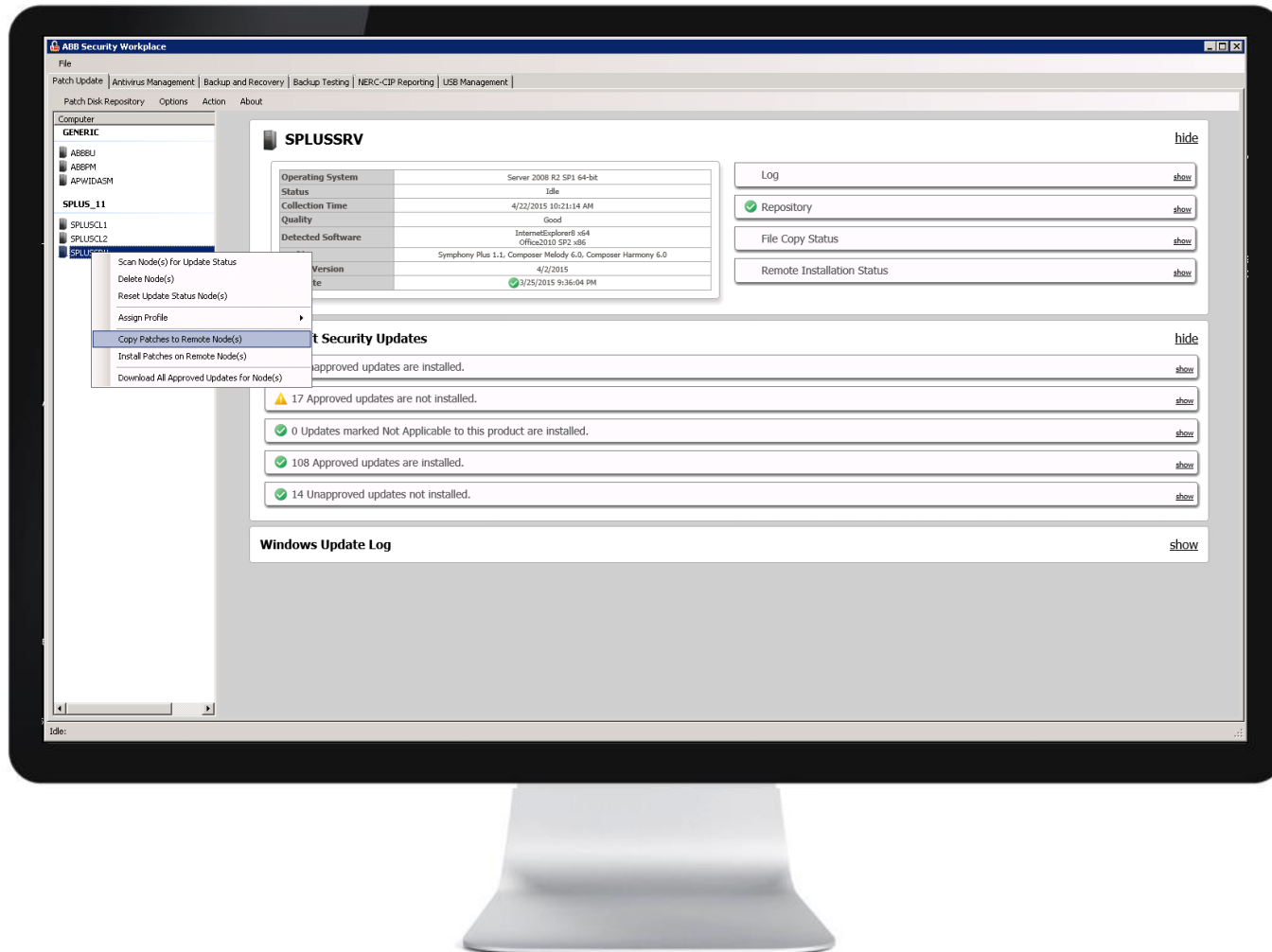


ABB Security Workplace Maintain - Demonstration

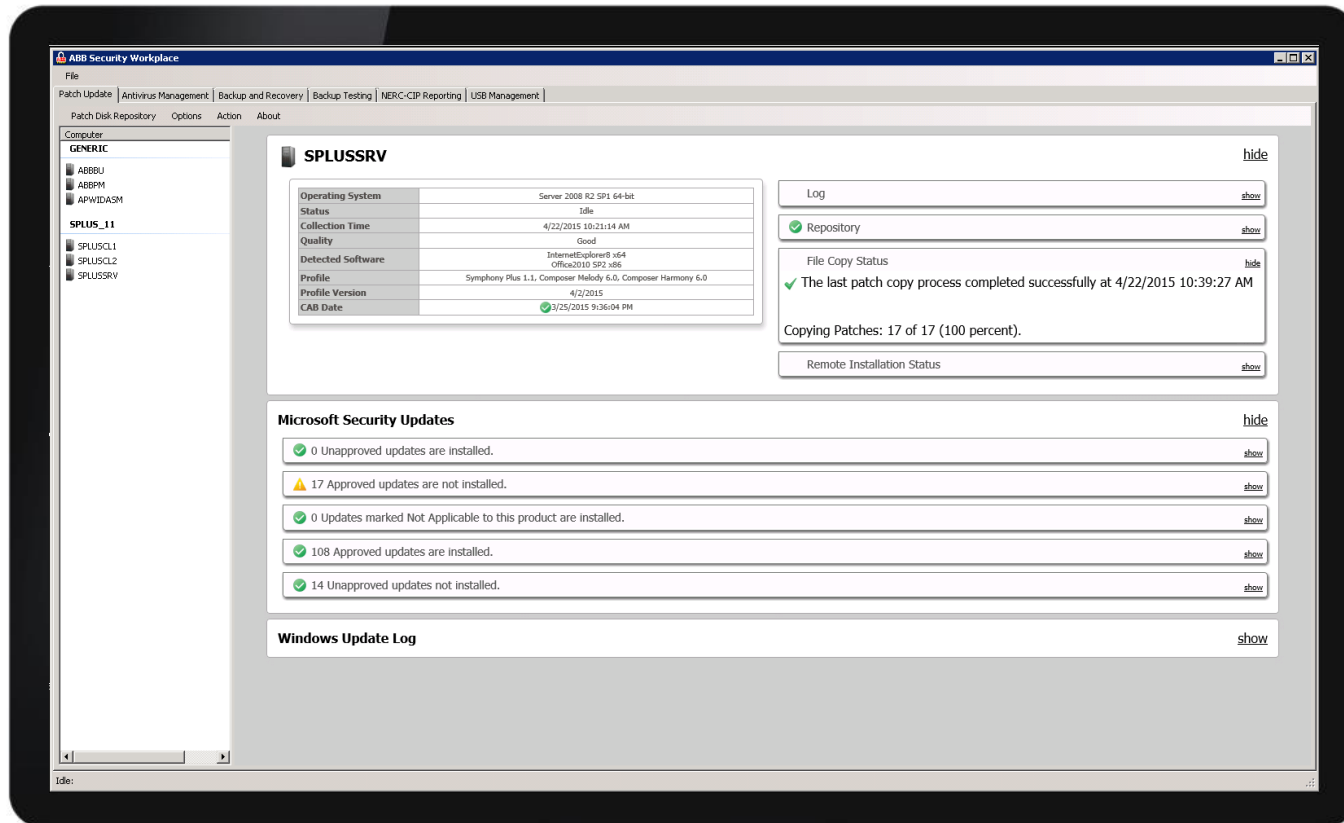


ABB Security Workplace Maintain - Demonstration

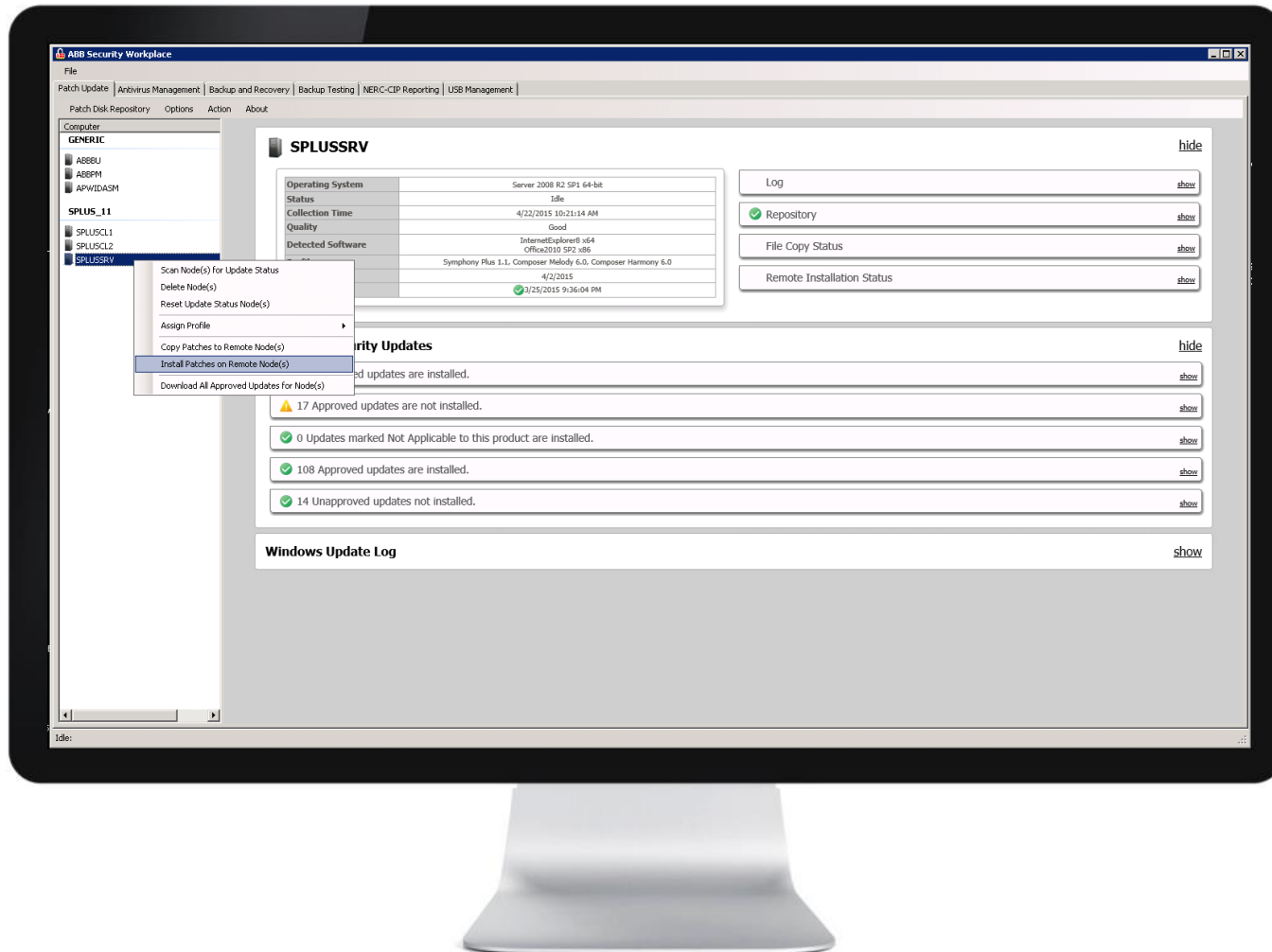


ABB Security Workplace Maintain - Demonstration

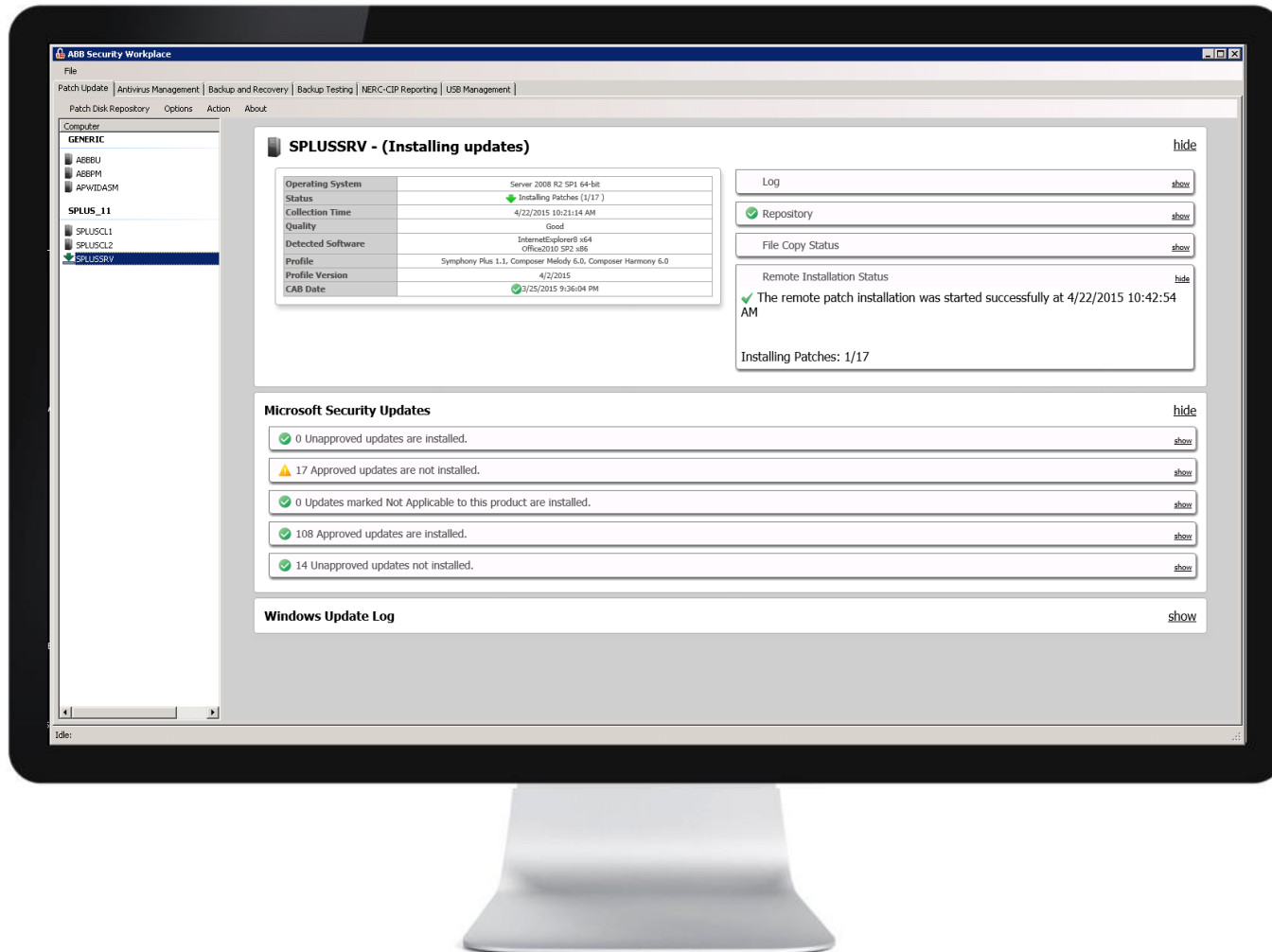


ABB Security Workplace Maintain - Demonstration

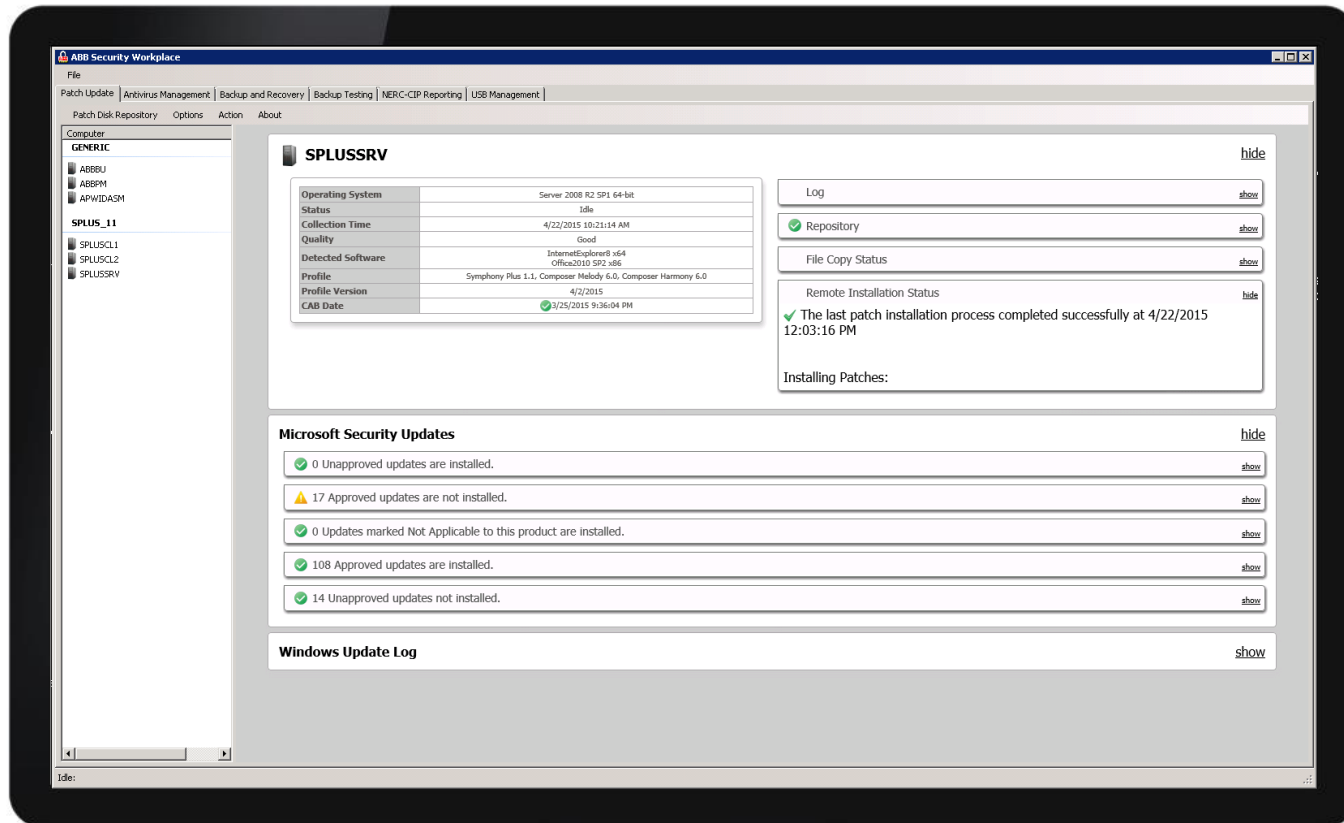


ABB Security Workplace Maintain - Demonstration



ABB Security Workplace Maintain - Demonstration

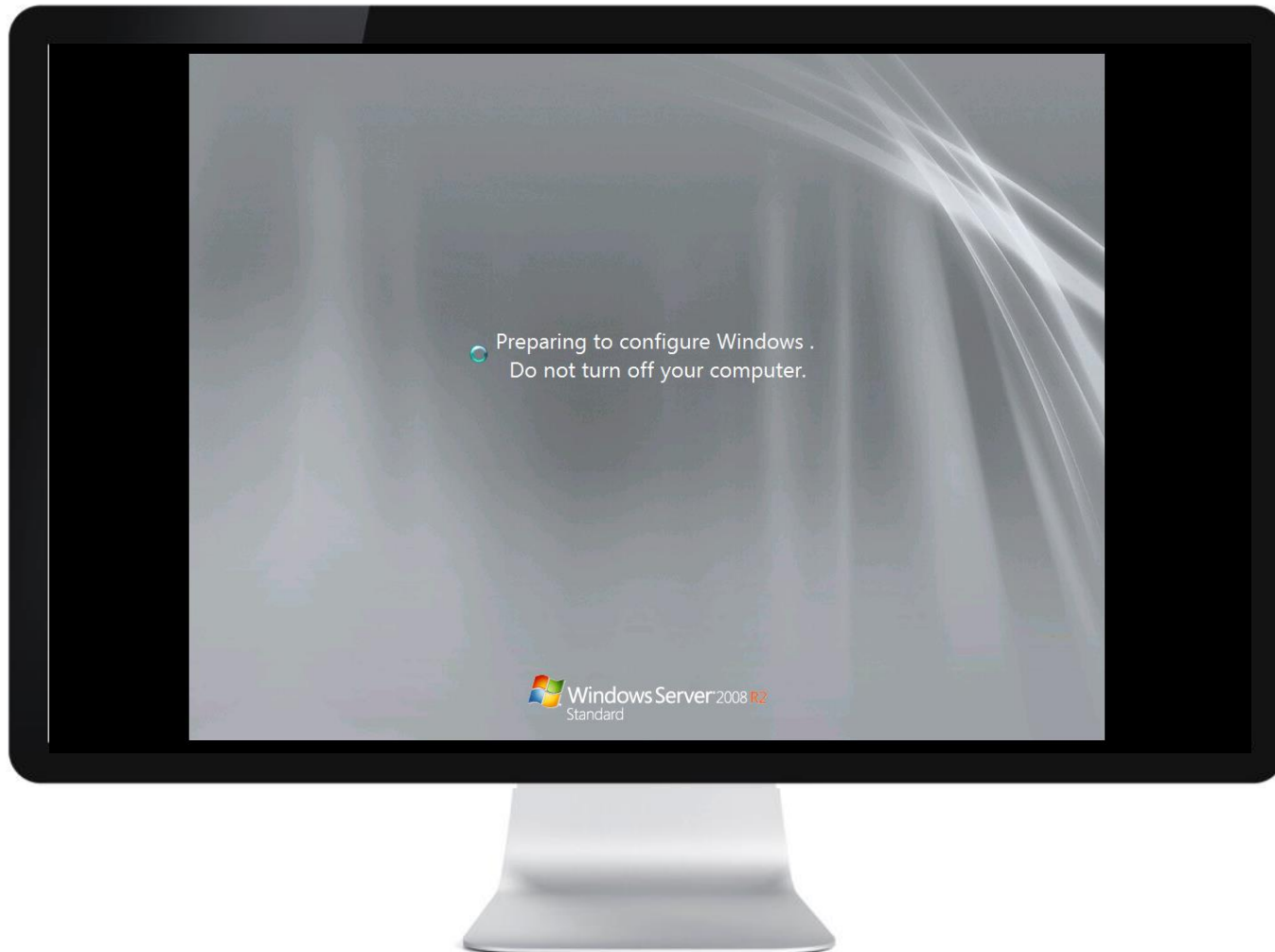


ABB Security Workplace Maintain - Demonstration



ABB Security Workplace Maintain - Demonstration

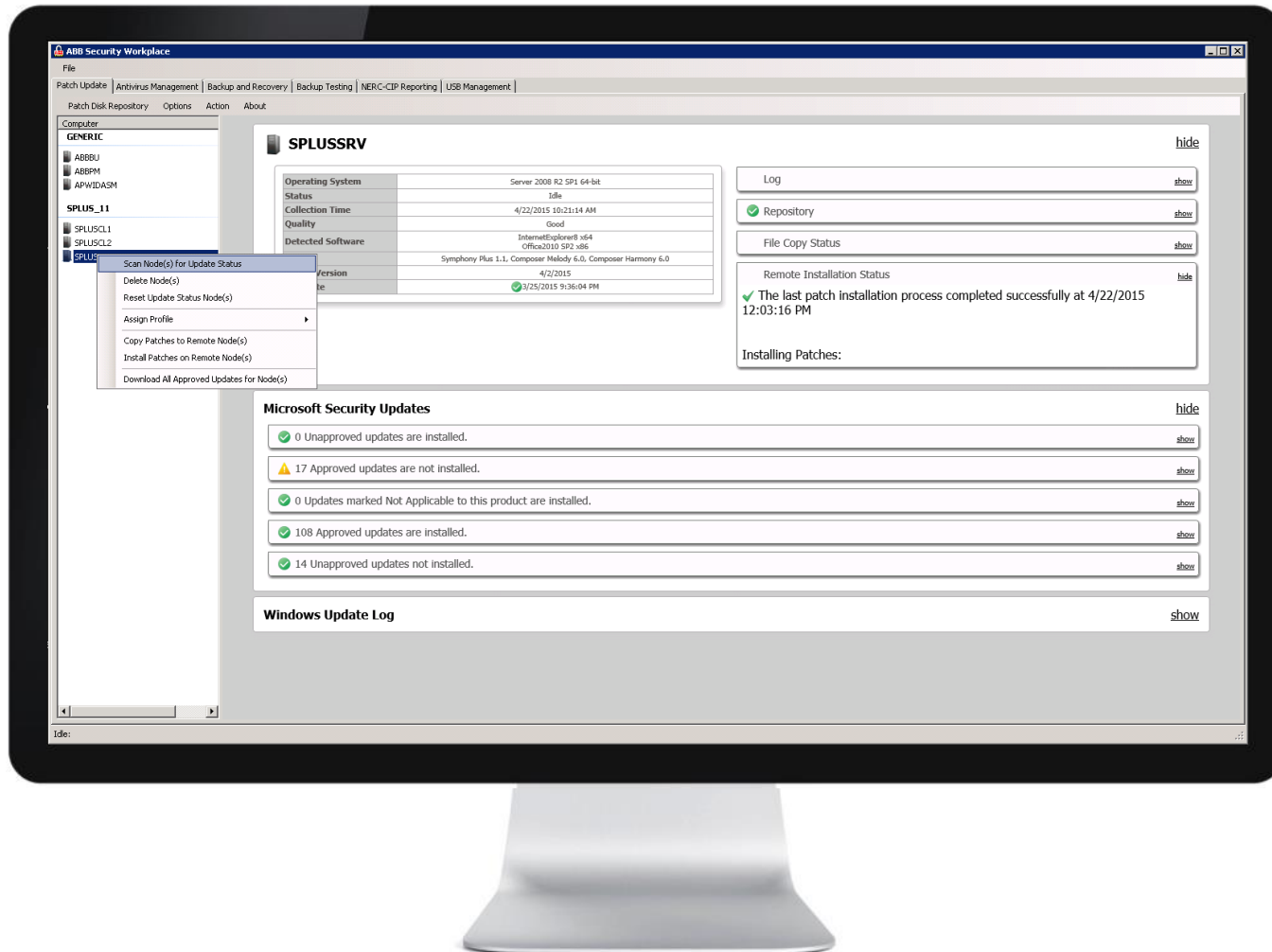


ABB Security Workplace Maintain - Demonstration

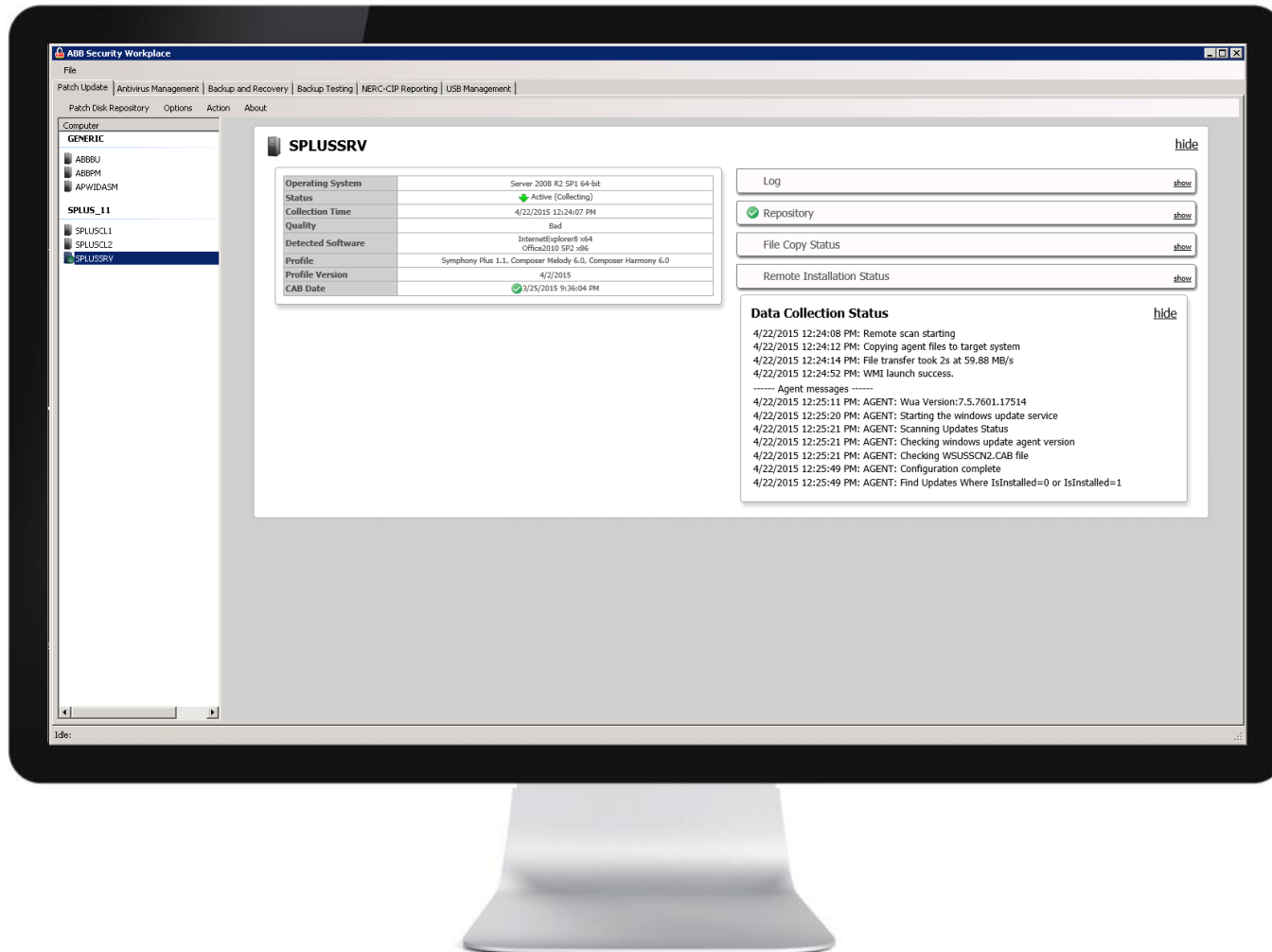


ABB Security Workplace Maintain - Demonstration

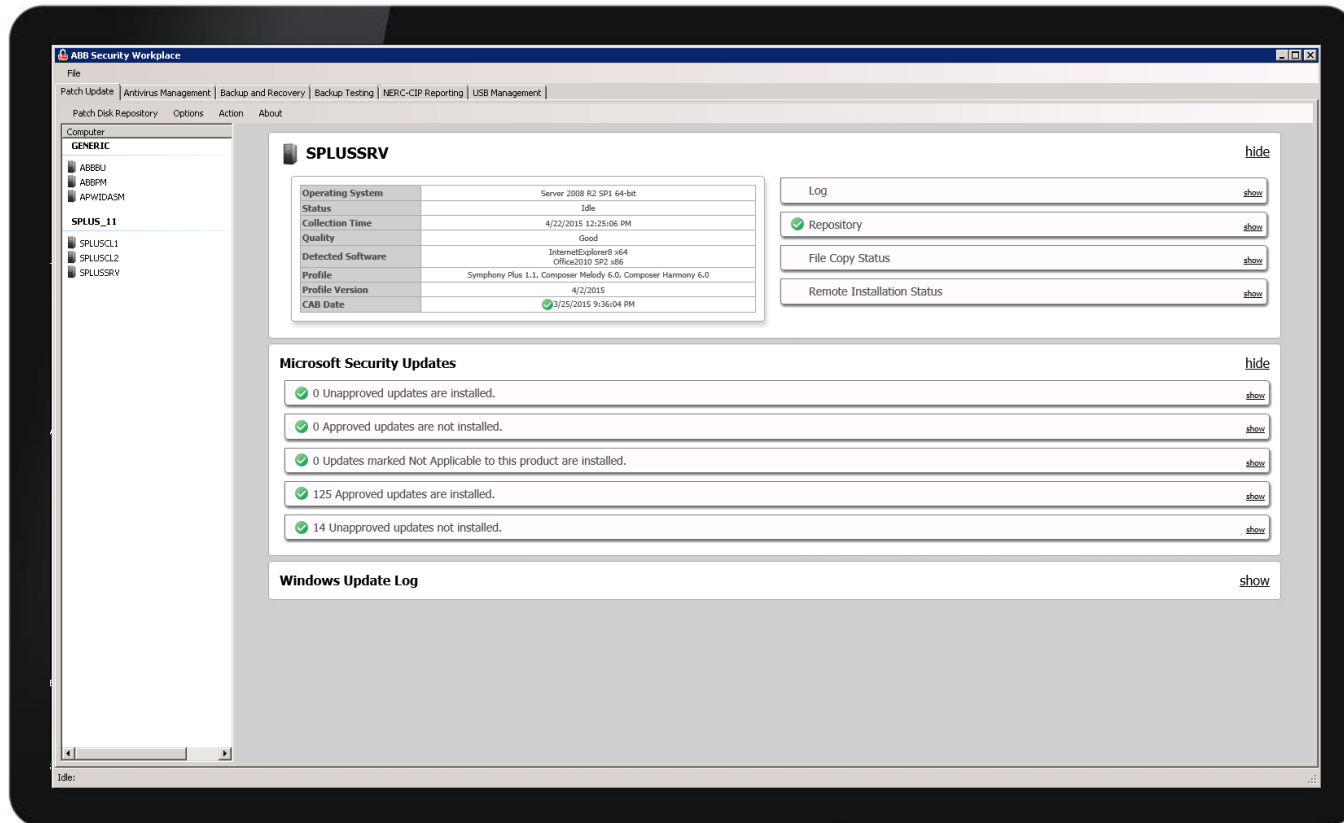


ABB Security Workplace Maintain - Demonstration

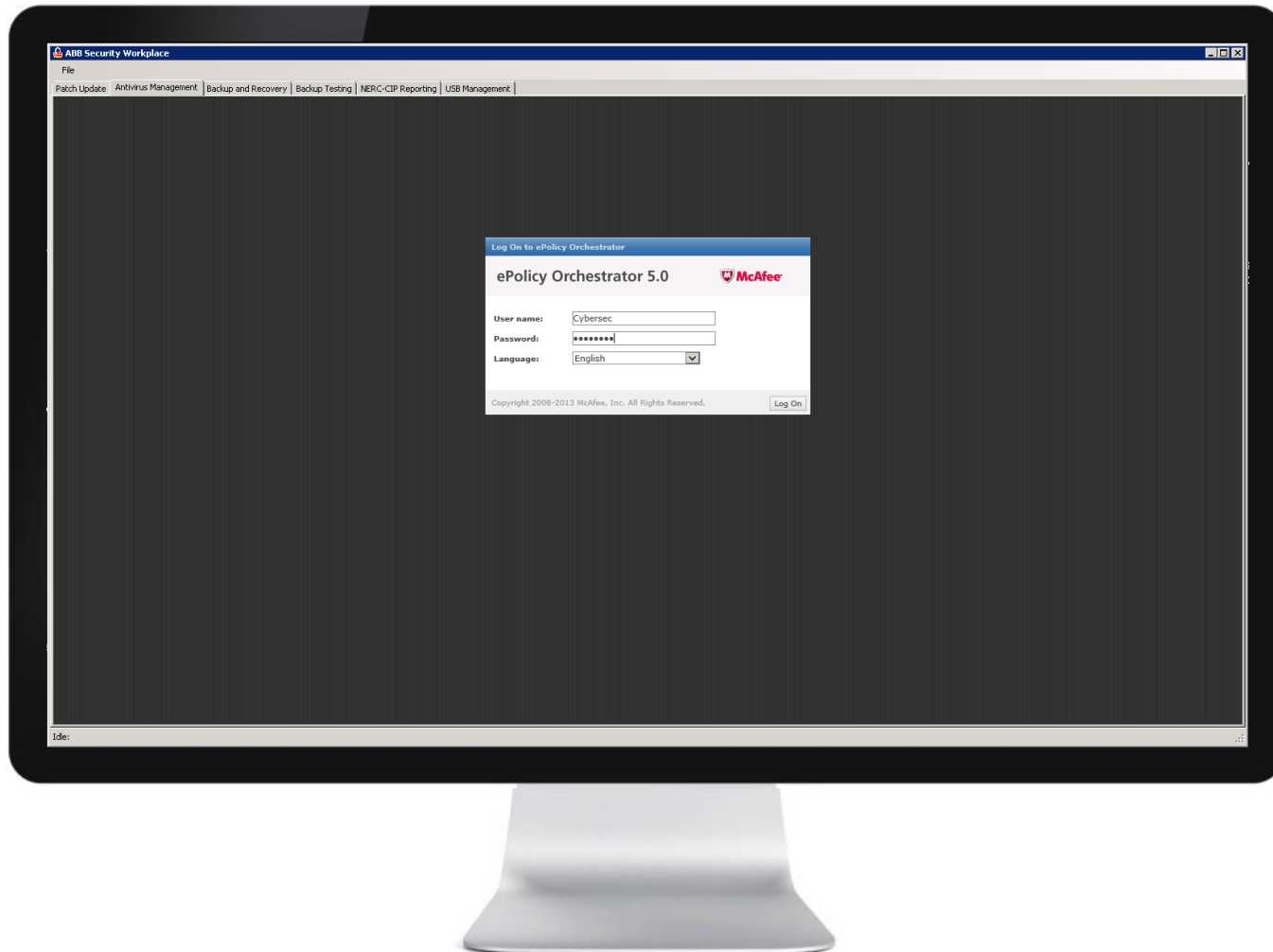


ABB Security Workplace Maintain - Demonstration

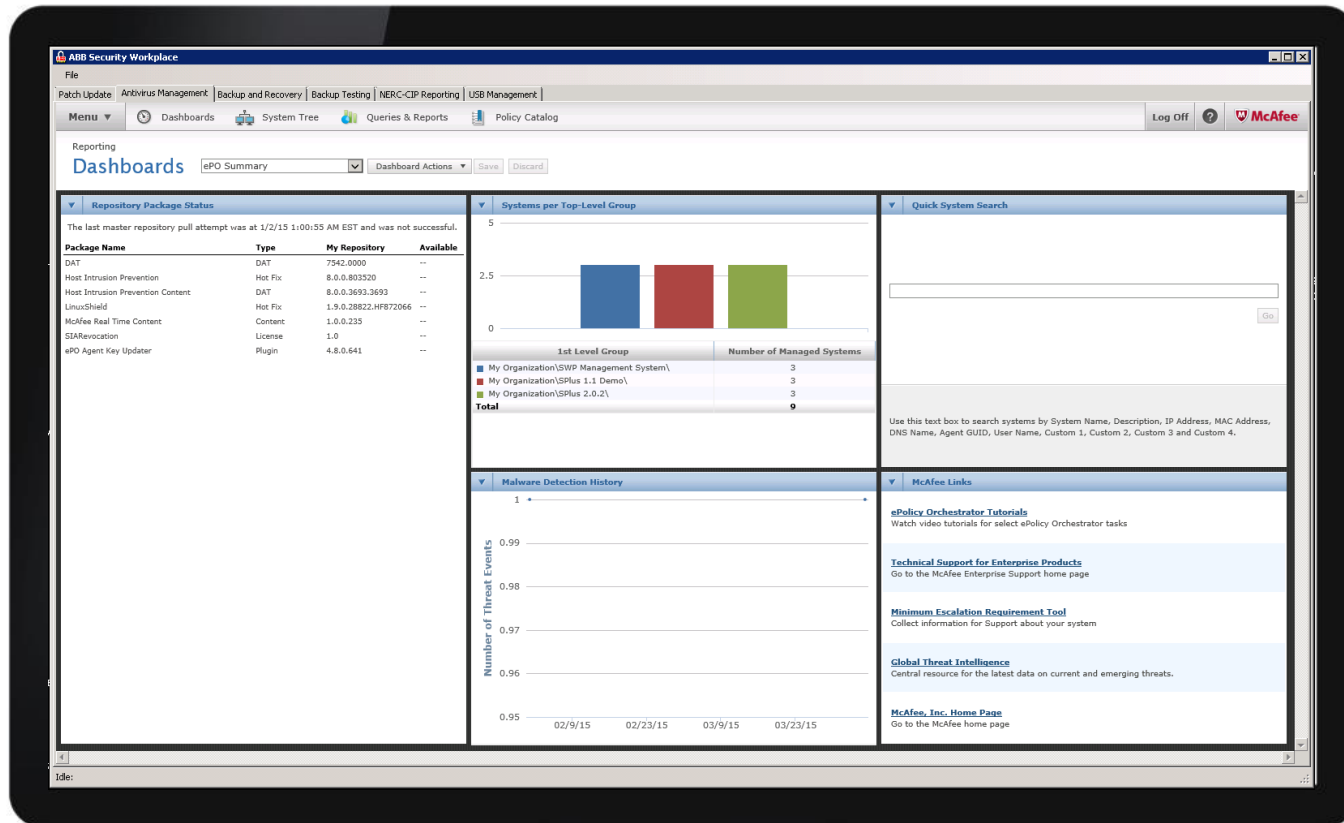


ABB Security Workplace Maintain - Demonstration

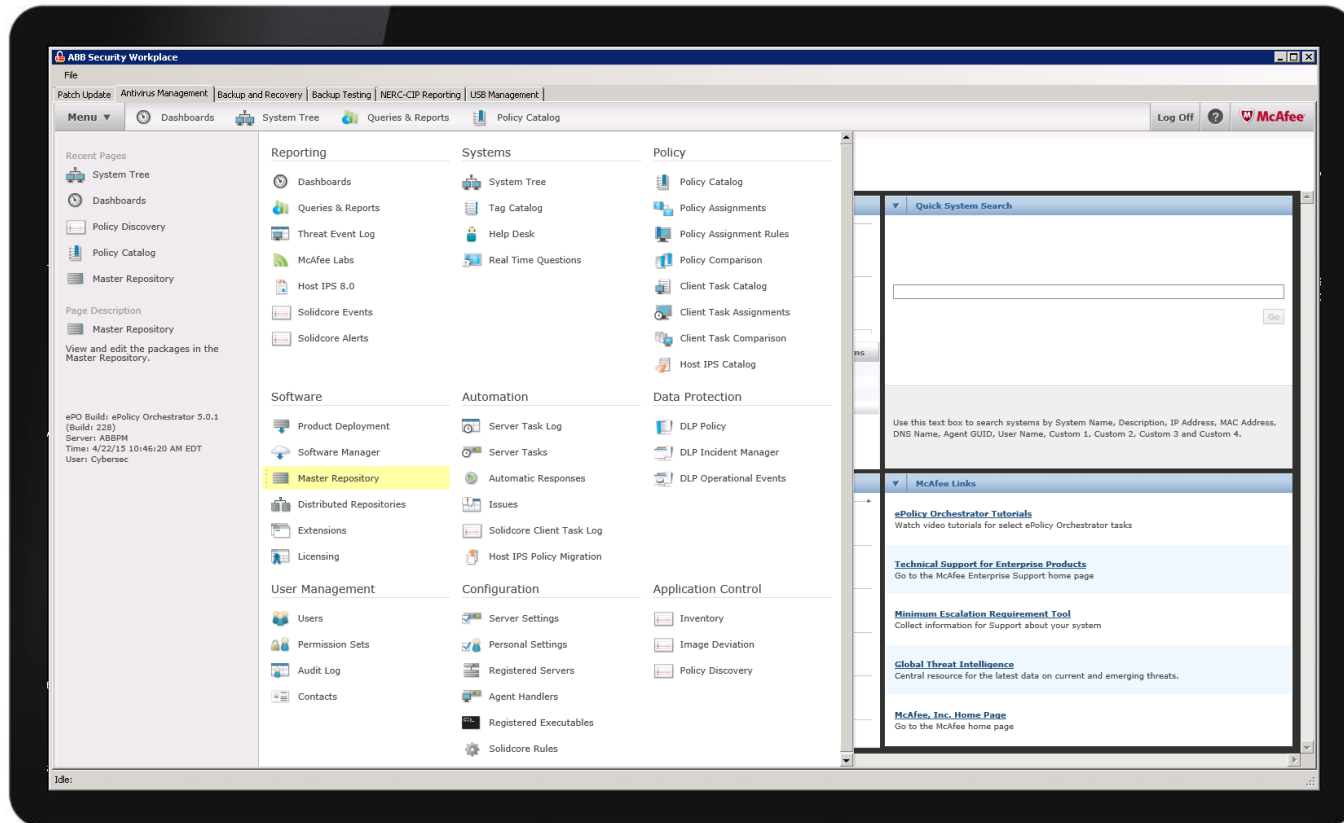


ABB Security Workplace Maintain - Demonstration



The screenshot displays the ABB Security Workplace Master Repository interface. The top navigation bar includes links for Patch Update, Antivirus Management, Backup and Recovery, Backup Testing, NERC-CIP Reporting, and USB Management. Below this is a menu bar with options like Dashboards, System Tree, Queries & Reports, and Policy Catalog. The main content area is titled 'Master Repository' and shows a list of packages in the Master Repository. The list includes columns for Name, Status, Type, Version, Minor Version, Language, Check-In Date, Signed by, Distribution Type, Branch, and Actions. The status of all packages is 'OK'. The actions column provides links to 'Change Branch' and 'Delete' for each package.

Name	Status	Type	Version	Minor Version	Language	Check-In Date	Signed by	Distribution Type	Branch	Actions
DAT	OK	DAT	7542.0000		Neutral	3/1/15 10:38:47 AM EST	McAfee		Current	Change Branch Delete
ePO Agent Key Updater	OK	Plugin	4.8.0	641	Neutral	4/11/14 3:29:34 PM EDT	ABBPM	Licensed	Current	Change Branch Delete
Host Intrusion Prevention	OK	Hot Fix	8.0.0	803520	Neutral	4/11/14 3:48:31 PM EDT	McAfee		Current	Change Branch Delete
Host Intrusion Prevention	OK	Install	8.0.0	2589	Neutral	4/11/14 3:48:14 PM EDT	McAfee	Licensed	Current	Change Branch Delete
Host Intrusion Prevention Content	OK	DAT	8.0.0	3693	Neutral	4/11/14 3:45:40 PM EDT	McAfee		Current	Change Branch Delete
LinuxShield	OK	Hot Fix	1.9.0.28822	HF872066	English	4/11/14 3:49:44 PM EDT	McAfee		Current	Change Branch Delete
McAfee Agent for Linux	OK	Install	4.8.0	641	English	4/11/14 3:29:52 PM EDT	ABBPM	Licensed	Current	Change Branch Delete
McAfee Agent for Mac OS X	OK	Install	4.8.0	887	English	4/11/14 3:52:06 PM EDT	ABBPM	Licensed	Current	Change Branch Delete
McAfee Agent for Windows	OK	Install	4.8.0	641	English	4/11/14 3:30:33 PM EDT	ABBPM	Licensed	Current	Change Branch Delete
McAfee Anti-Spam for McAfee Security for M	OK	Install	8.0.0	7905	Neutral	4/11/14 3:50:32 PM EDT	McAfee		Current	Change Branch Delete
McAfee Data Loss Prevention	OK	Install	9.3.0	637	English	4/11/14 3:47:49 PM EDT	McAfee		Current	Change Branch Delete
McAfee Endpoint Protection for Mac	OK	Install	2.1.0	1085	Neutral	4/11/14 3:48:59 PM EDT	McAfee		Current	Change Branch Delete
McAfee ePO Deep Command Discovery Plugi	OK	Install	2.0.0	437	Neutral	4/11/14 3:44:15 PM EDT	ABBPM	Licensed	Current	Change Branch Delete
McAfee Quarantine Manager	OK	Install	7.0.1	1266	Neutral	4/11/14 3:50:51 PM EDT	McAfee		Current	Change Branch Delete
McAfee Real Time Client	OK	Install	1.0.1	111	Neutral	4/11/14 3:51:32 PM EDT	ABBPM	Licensed	Current	Change Branch Delete
McAfee Real Time Content	OK	Content	1.0.0	235	Neutral	4/11/14 3:51:49 PM EDT	ABBPM		Current	Change Branch Delete
McAfee Security for Microsoft Exchange (x64	OK	Install	8.0.0	7905	Neutral	4/11/14 3:50:15 PM EDT	McAfee		Current	Change Branch Delete
MySQL for McAfee Quarantine Manager	OK	Install	7.0.1	1266	Neutral	4/11/14 3:51:12 PM EDT	McAfee		Current	Change Branch Delete
Product Improvement Program	OK	Install	1.1.0	485	Neutral	4/11/14 3:29:45 PM EDT	McAfee	Licensed	Current	Change Branch Delete
SiteAdvisor Enterprise	OK	Install	3.5.0	1121	Neutral	4/11/14 3:47:21 PM EDT	McAfee		Current	Change Branch Delete
Solidcore Client for Windows	OK	Install	6.1.3	392	Neutral	2/5/15 11:57:23 AM EST	ABBPM	Licensed	Current	Change Branch Delete
VirusScan Enterprise	OK	Install	8.8.0	1128	Neutral	4/11/14 3:47:04 PM EDT	McAfee	Licensed	Current	Change Branch Delete
VirusScan Enterprise for Linux	OK	Install	1.9.0	28822	English	4/11/14 3:49:25 PM EDT	McAfee		Current	Change Branch Delete

At the bottom of the interface, there is an 'Actions' dropdown menu showing '23 items', a 'Pull Now' button, and a 'Check In Package' button. The status bar at the very bottom indicates 'Idle'.

ABB Security Workplace Maintain - Demonstration

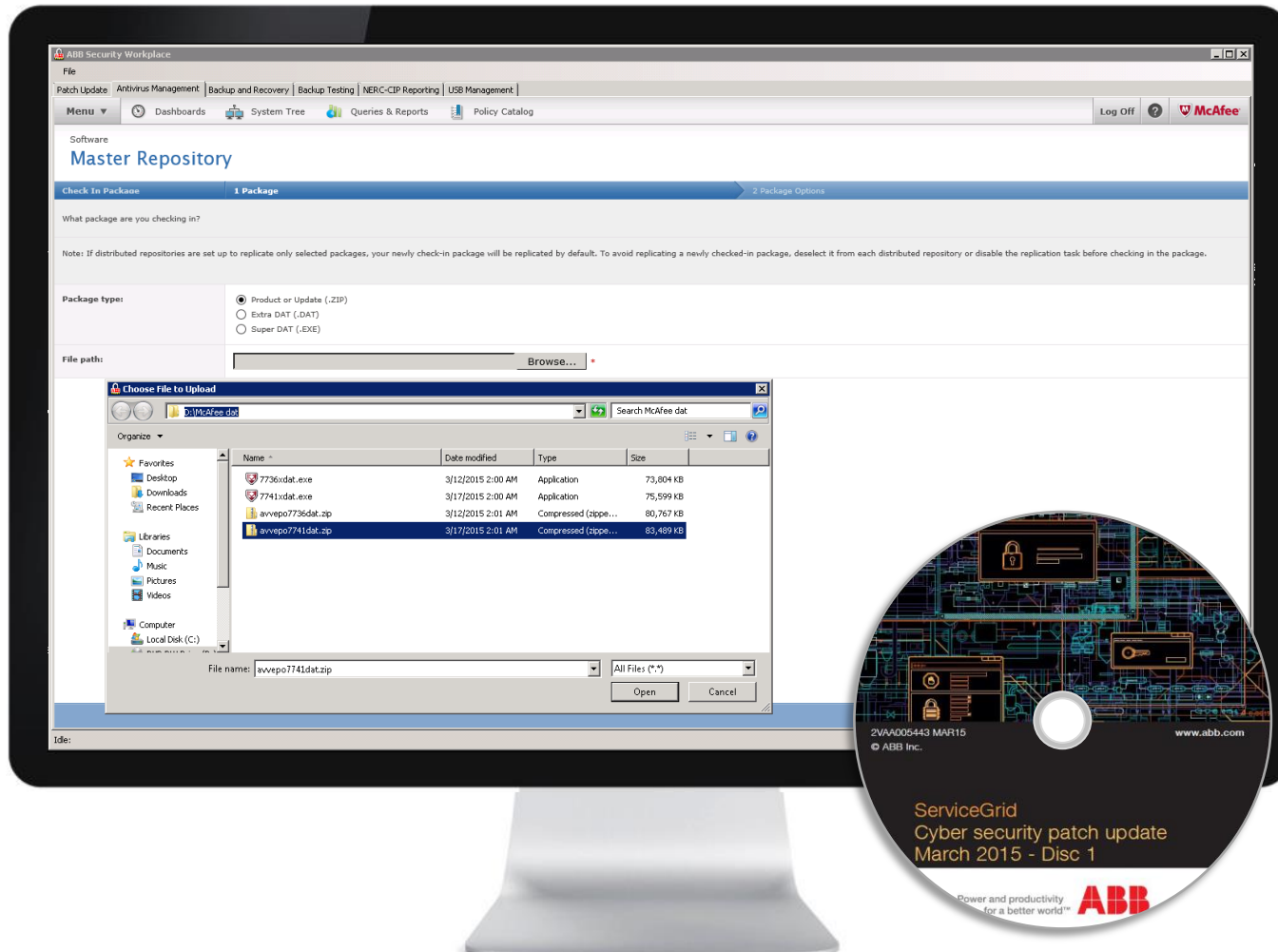


ABB Security Workplace Maintain - Demonstration

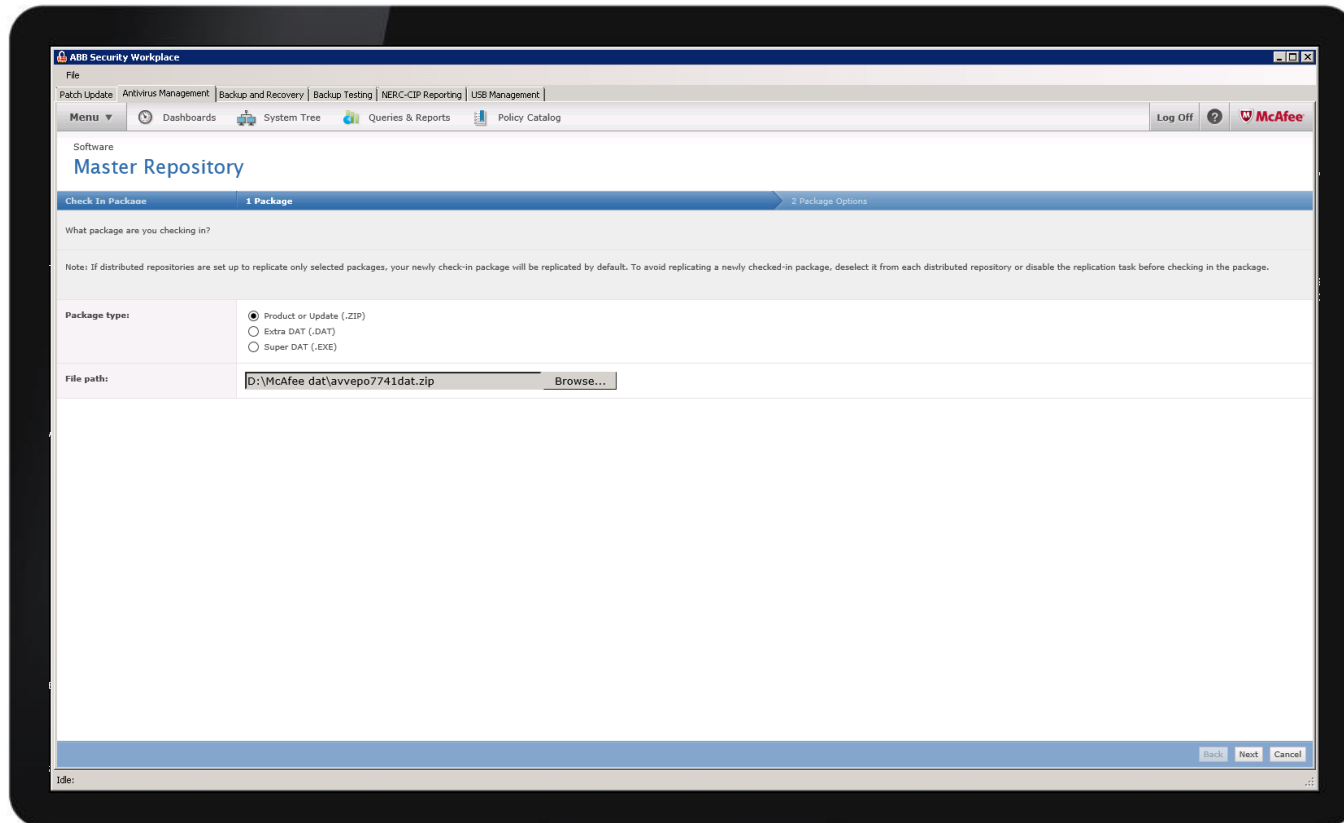


ABB Security Workplace Maintain - Demonstration

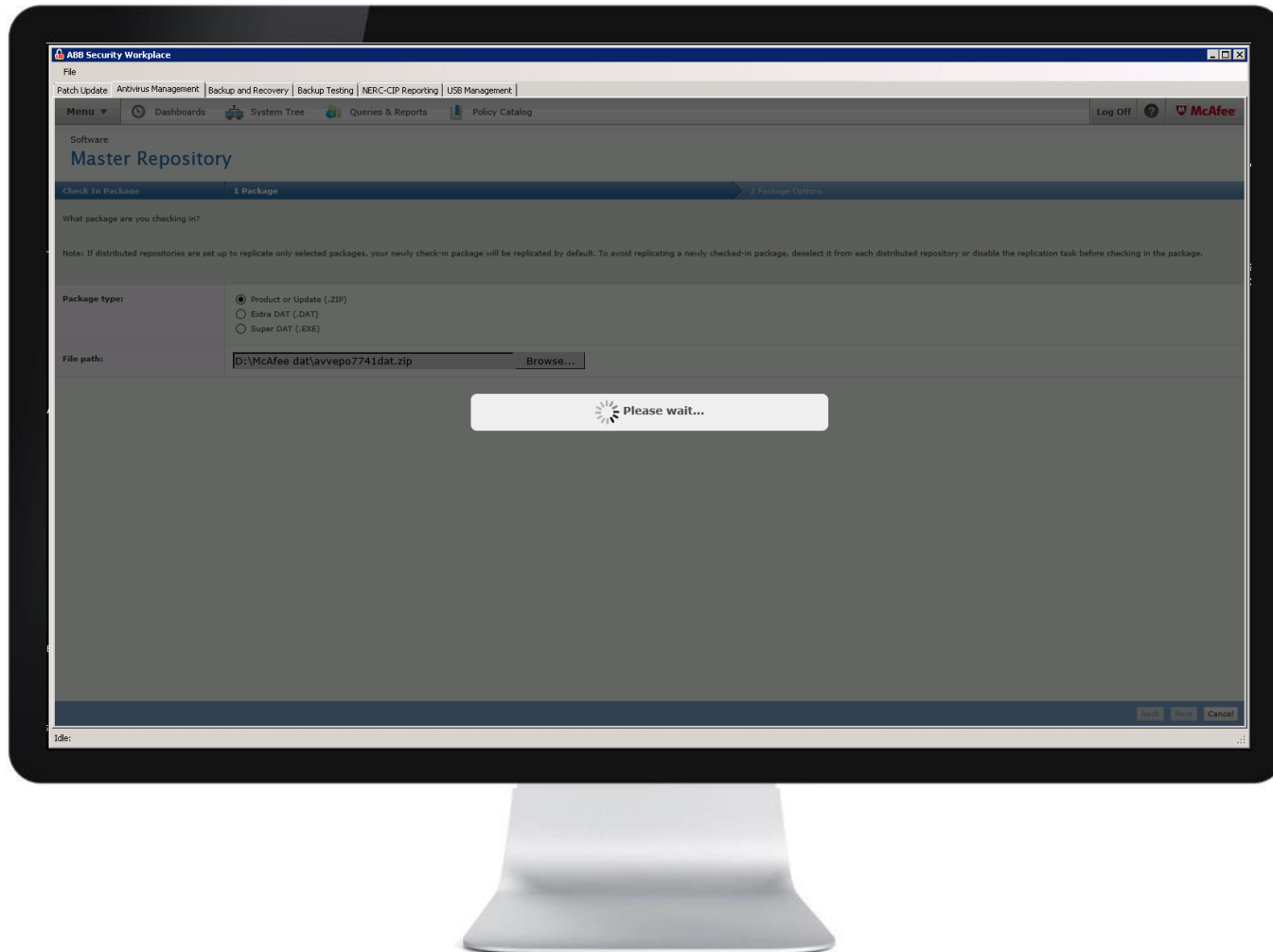


ABB Security Workplace Maintain - Demonstration

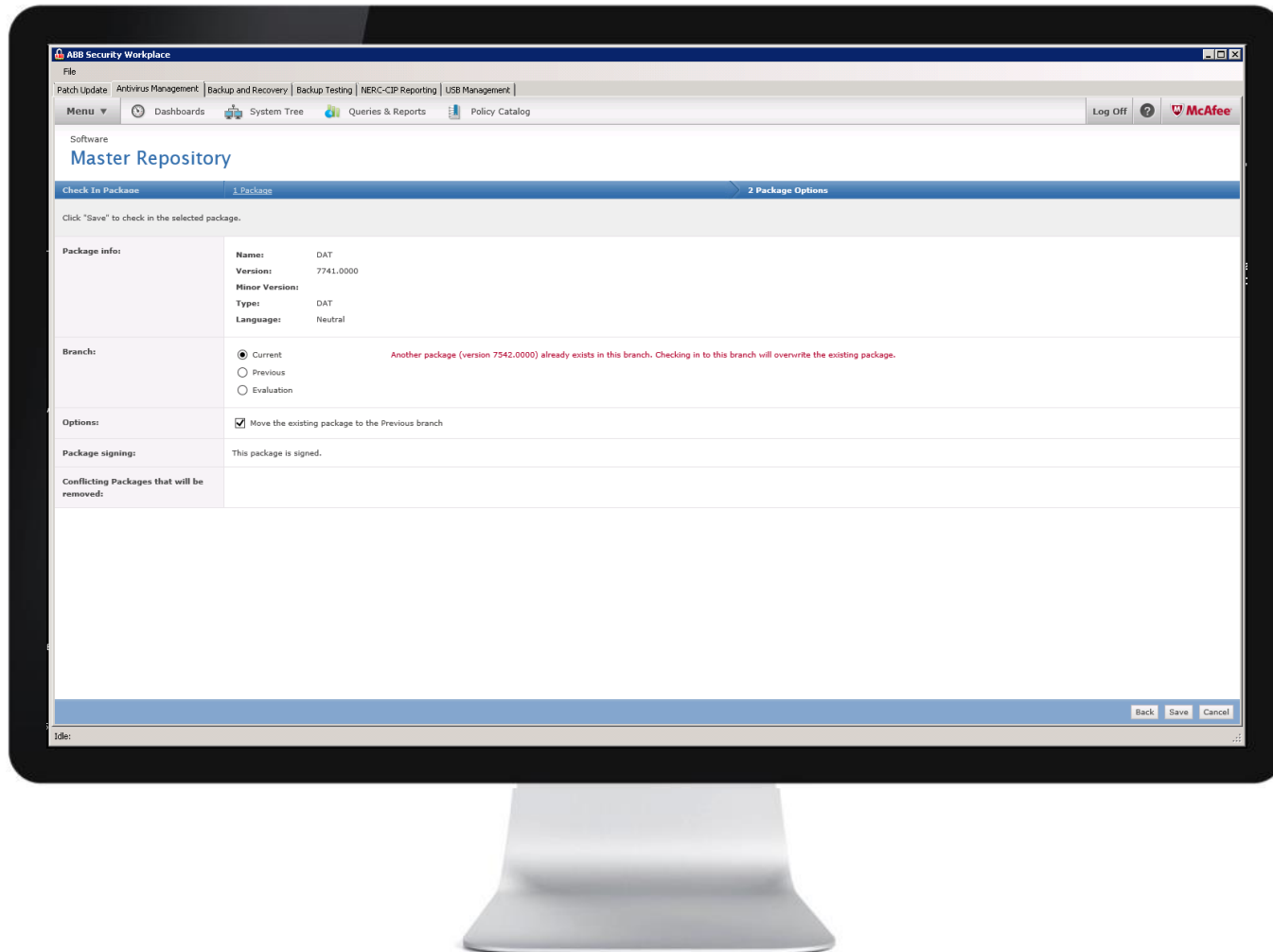


ABB Security Workplace Maintain - Demonstration



The screenshot displays the ABB Security Workplace Master Repository interface. The top navigation bar includes links for Patch Update, Antivirus Management, Backup and Recovery, Backup Testing, NERC-CIP Reporting, and USB Management. Below this, a menu bar shows Dashboards, System Tree, Queries & Reports, and Policy Catalog. The main content area is titled "Master Repository" and shows a list of packages in the Master Repository. The list includes columns for Name, Status, Type, Version, Minor Version, Language, Check-In Date, Signed by, Distribution Type, Branch, and Actions. The packages listed include DAT, ePO Agent Key Updater, Host Intrusion Prevention, LinuxShield, McAfee Agent for Linux, McAfee Agent for Mac OS X, McAfee Agent for Windows, McAfee Anti-Spam for McAfee Security for M, McAfee Data Loss Prevention, McAfee Endpoint Protection for Mac, McAfee ePO Deep Command Discovery Plug, McAfee Quarantine Manager, McAfee Real Time Client, McAfee Real Time Content, McAfee Security for Microsoft Exchange (x64), MySQL for McAfee Quarantine Manager, Product Improvement Program, SiteAdvisor Enterprise, Solidcore Client for Windows, and VirusScan Enterprise.

Name	Status	Type	Version	Minor Version	Language	Check-In Date	Signed by	Distribution Type	Branch	Actions
DAT	OK	DAT	7741.0000		Neutral	4/22/15 10:54:29 AM EDT	McAfee		Current	Change Branch Delete
DAT	OK	DAT	7542.0000		Neutral	4/22/15 10:54:25 AM EDT	McAfee		Previous	Change Branch Delete
ePO Agent Key Updater	OK	Plugin	4.8.0	641	Neutral	4/11/14 3:29:34 PM EDT	ABBPM	Licensed	Current	Change Branch Delete
Host Intrusion Prevention	OK	Hot Fix	8.0.0	803520	Neutral	4/11/14 3:48:31 PM EDT	McAfee		Current	Change Branch Delete
Host Intrusion Prevention	OK	Install	8.0.0	2589	Neutral	4/11/14 3:48:14 PM EDT	McAfee	Licensed	Current	Change Branch Delete
Host Intrusion Prevention Content	OK	DAT	8.0.0	3693	Neutral	4/11/14 3:45:40 PM EDT	McAfee		Current	Change Branch Delete
LinuxShield	OK	Hot Fix	1.9.0.28822	HF872066	English	4/11/14 3:49:44 PM EDT	McAfee		Current	Change Branch Delete
McAfee Agent for Linux	OK	Install	4.8.0	641	English	4/11/14 3:29:52 PM EDT	ABBPM	Licensed	Current	Change Branch Delete
McAfee Agent for Mac OS X	OK	Install	4.8.0	887	English	4/11/14 3:52:08 PM EDT	ABBPM	Licensed	Current	Change Branch Delete
McAfee Agent for Windows	OK	Install	4.8.0	641	English	4/11/14 3:30:33 PM EDT	ABBPM	Licensed	Current	Change Branch Delete
McAfee Anti-Spam for McAfee Security for M	OK	Install	8.0.0	7905	Neutral	4/11/14 3:50:32 PM EDT	McAfee		Current	Change Branch Delete
McAfee Data Loss Prevention	OK	Install	9.3.0	637	English	4/11/14 3:47:49 PM EDT	McAfee		Current	Change Branch Delete
McAfee Endpoint Protection for Mac	OK	Install	2.1.0	1085	Neutral	4/11/14 3:48:59 PM EDT	McAfee		Current	Change Branch Delete
McAfee ePO Deep Command Discovery Plug	OK	Install	2.0.0	437	Neutral	4/11/14 3:44:15 PM EDT	ABBPM	Licensed	Current	Change Branch Delete
McAfee Quarantine Manager	OK	Install	7.0.1	1266	Neutral	4/11/14 3:50:51 PM EDT	McAfee		Current	Change Branch Delete
McAfee Real Time Client	OK	Install	1.0.1	111	Neutral	4/11/14 3:51:32 PM EDT	ABBPM	Licensed	Current	Change Branch Delete
McAfee Real Time Content	OK	Content	1.0.0	235	Neutral	4/11/14 3:51:49 PM EDT	ABBPM		Current	Change Branch Delete
McAfee Security for Microsoft Exchange (x64	OK	Install	8.0.0	7905	Neutral	4/11/14 3:50:15 PM EDT	McAfee		Current	Change Branch Delete
MySQL for McAfee Quarantine Manager	OK	Install	7.0.1	1266	Neutral	4/11/14 3:51:12 PM EDT	McAfee		Current	Change Branch Delete
Product Improvement Program	OK	Install	1.1.0	485	Neutral	4/11/14 3:29:45 PM EDT	McAfee	Licensed	Current	Change Branch Delete
SiteAdvisor Enterprise	OK	Install	3.5.0	1121	Neutral	4/11/14 3:47:21 PM EDT	McAfee		Current	Change Branch Delete
Solidcore Client for Windows	OK	Install	6.1.3	392	Neutral	2/5/15 11:57:23 AM EST	ABBPM	Licensed	Current	Change Branch Delete
VirusScan Enterprise	OK	Install	8.8.0	1128	Neutral	4/11/14 3:47:04 PM EDT	McAfee	Licensed	Current	Change Branch Delete

Actions: 24 items | Pull Now | Check In Package

ABB Security Workplace Maintain - Demonstration

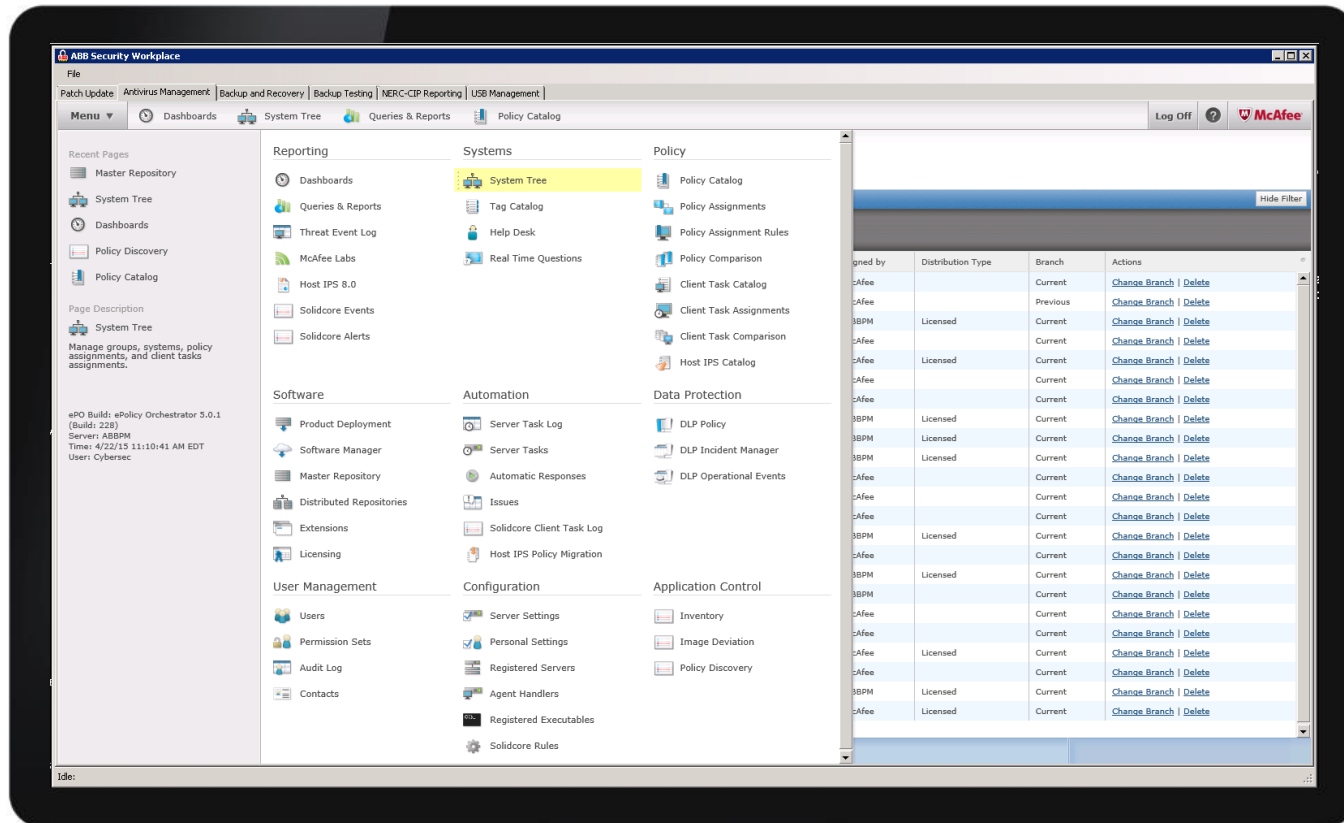


ABB Security Workplace Maintain - Demonstration

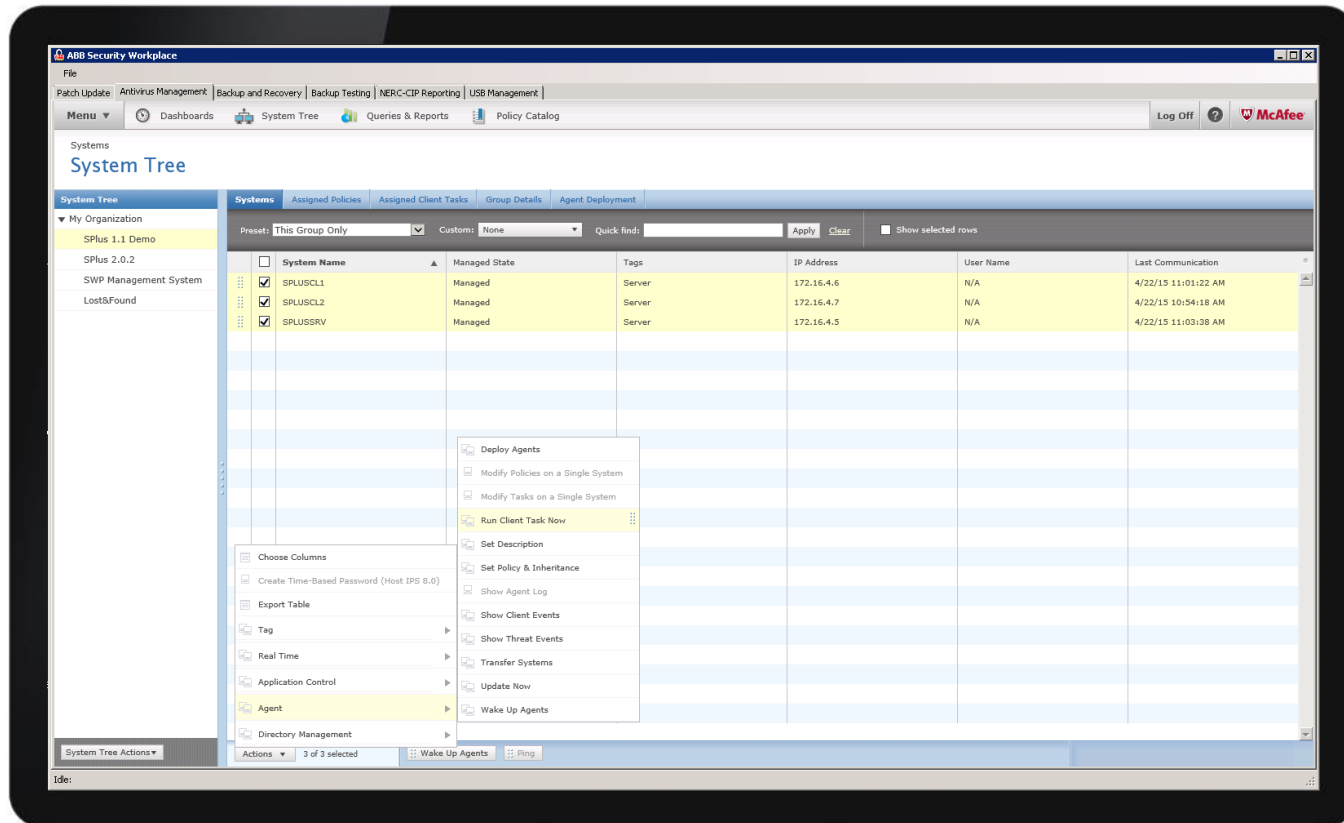


ABB Security Workplace Maintain - Demonstration

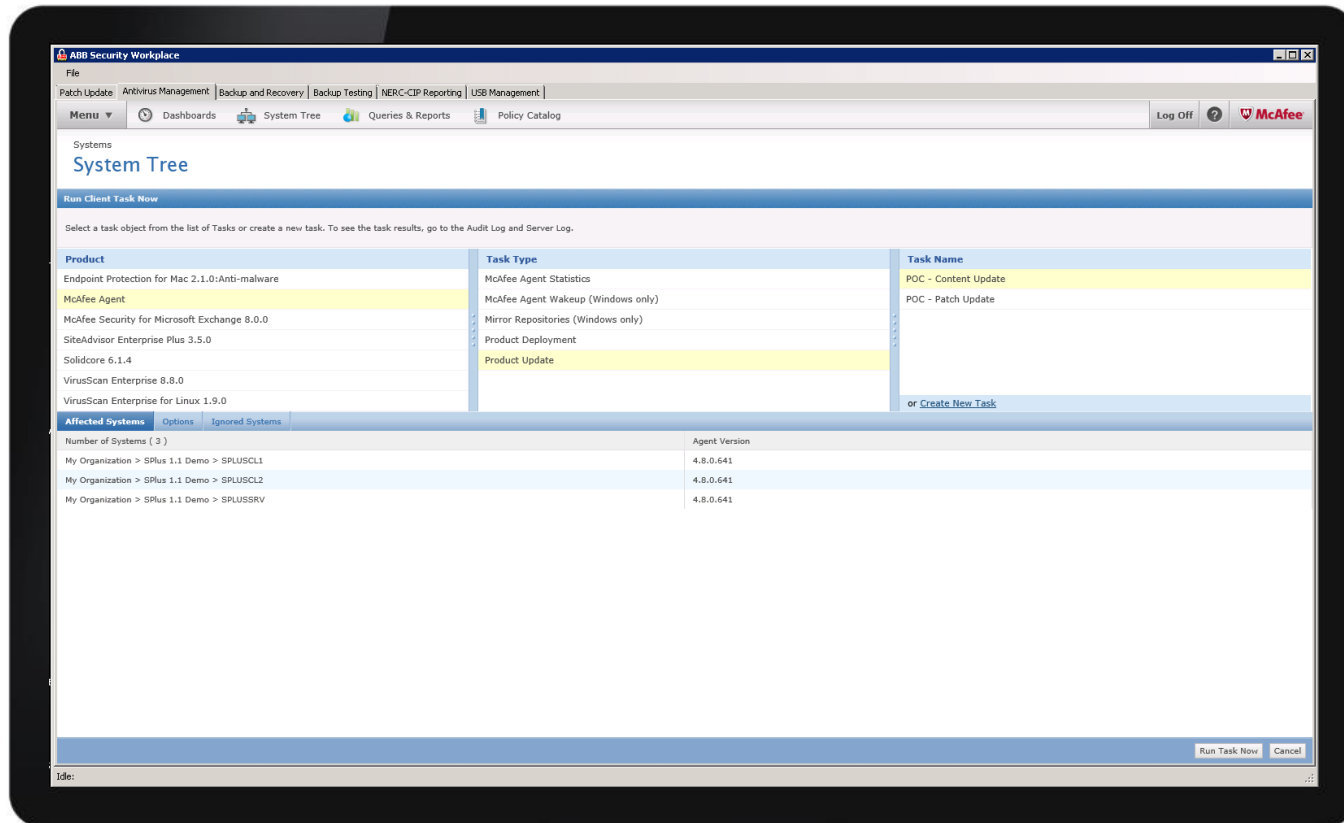


ABB Security Workplace Maintain - Demonstration

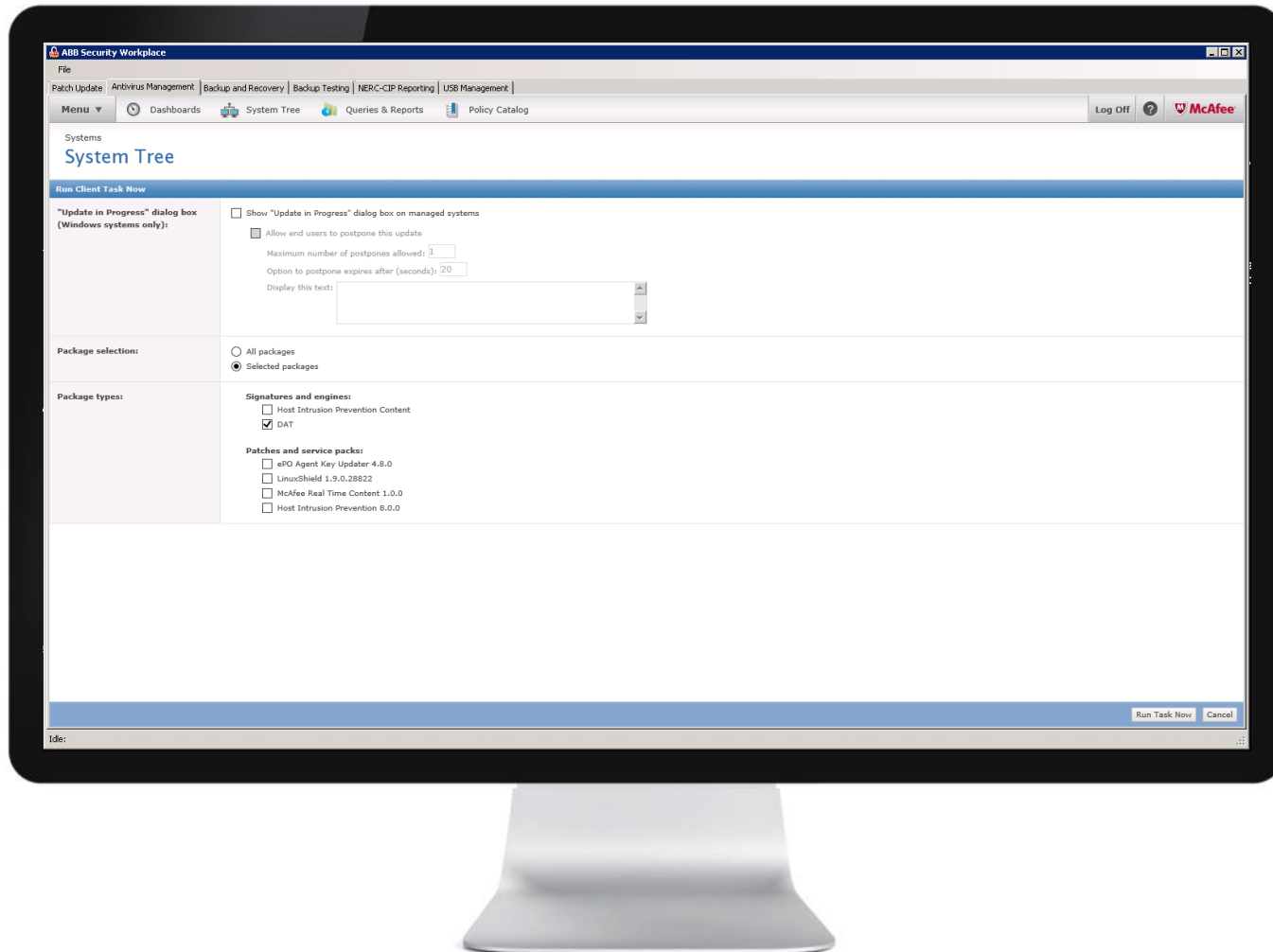


ABB Security Workplace Maintain - Demonstration

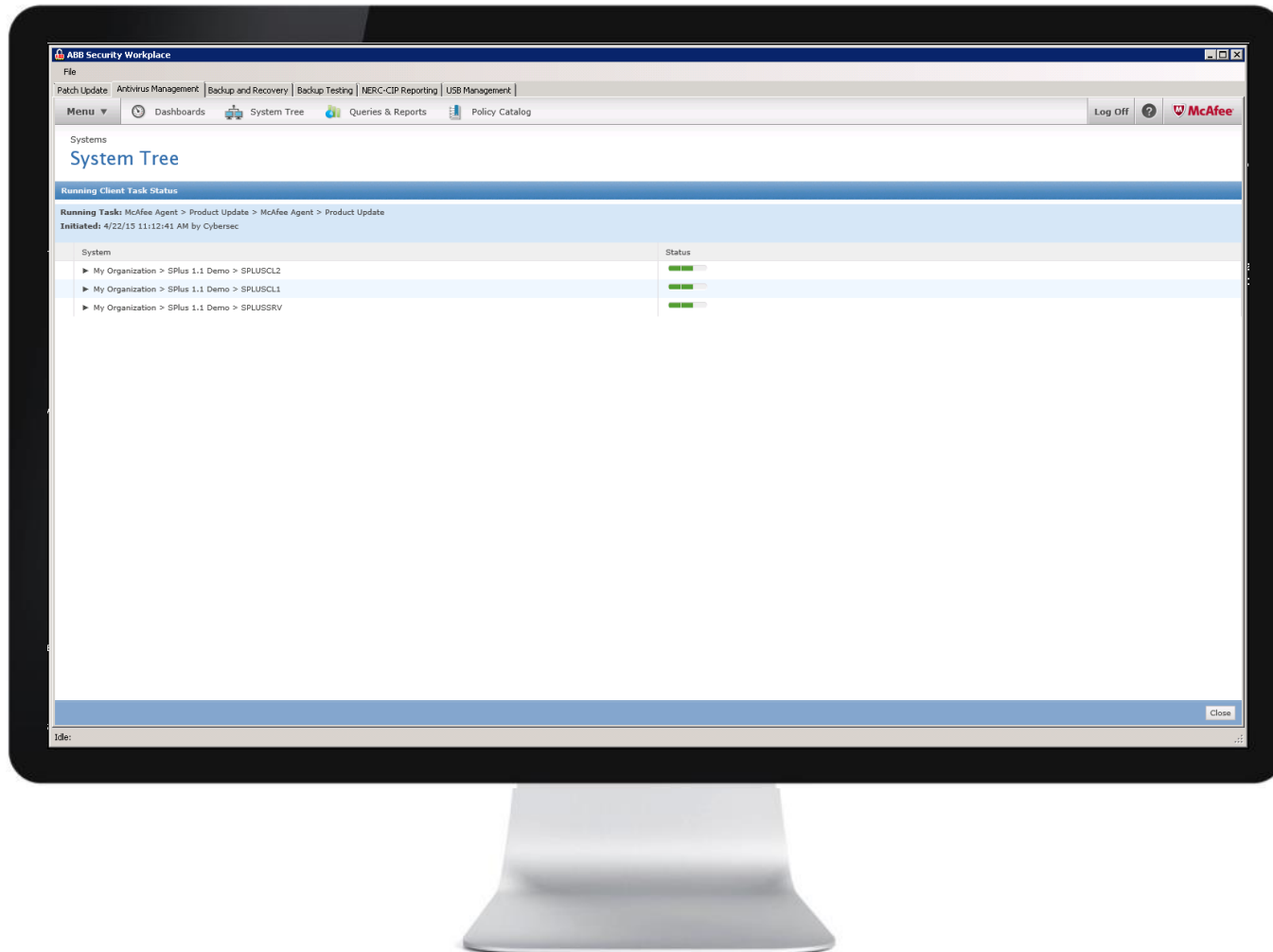


ABB Security Workplace Maintain - Demonstration



**Power and productivity
for a better world™**

