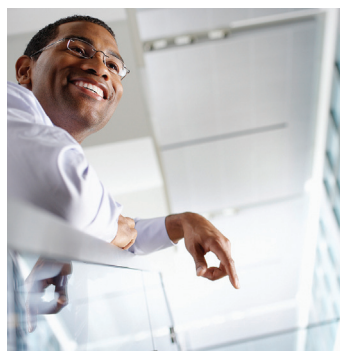


Incident Response and Forensics

Enable forensic analysis on assets managed by McAfee ePolicy Orchestrator

Now you can conduct fine-grained digital investigations on assets managed by McAfee® ePolicy Orchestrator® (McAfee ePO™)—McAfee’s centralized management framework—using forensic analysis technology from AccessData. McAfee and AccessData have created an integrated solution that extends the reach of McAfee system security for the endpoint.



McAfee Compatible Solution

- AccessData 1.1.0 agent and McAfee ePO 4.0 and 4.5

Business Problem

The demand for forensic investigations is rapidly growing at government and commercial organizations of all sizes. The ability to conduct digital investigations has become an essential capability for incident response, information assurance, classified message recovery, and e-discovery. Security experts require enterprise-class tools for thorough, inexpensive, and “forensically sound” investigations across the network.

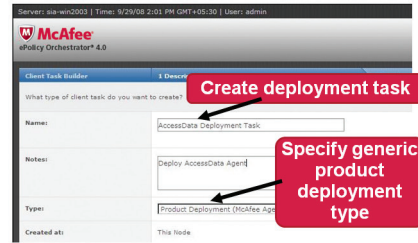
McAfee and AccessData Joint Solution and Benefits

McAfee has partnered with AccessData to bring powerful computer forensics, incident response, and e-discovery capabilities to McAfee customers. AccessData has pioneered digital investigations for 20 years, providing the technology and training that empower law enforcement, government agencies, and corporations to perform computer investigations with speed and efficiency.

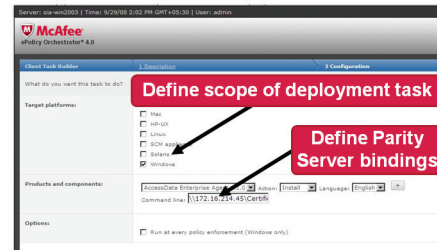
This joint, integrated solution allows ePO administrators to do the following:

- Use McAfee ePO to deploy AccessData agents on McAfee ePO-managed assets
- View agent coverage reports that include publisher, product, version, and more
- AccessData facilitates e-discovery, incident response, and forensic investigations:
 - » *E-Discovery*—Automate every part of the e-discovery process from collection to production, saving time and money for each significant incident
 - » *Incident Response*—AccessData Enterprise enables quick investigations of hacking incidents and malware in volatile data on target machines across the network
 - » *Forensic Investigations*—AccessData Enterprise allows an examiner to probe employee computer use for policy violations or IP theft
- With AccessData, you can perform the following basic technical operations:
 - » Remotely investigate target computers across the network undetected by the end users. Forensically acquire and analyze target files, entire drives, and RAM.
 - » Recover deleted data and files in unallocated and slack space, as well as decrypt documents and crack passwords
 - » Search target nodes against any search criteria including keywords, file types, user, or any metadata
- McAfee ePO enhances the forensic effort by correlating users in its database with assets or activities under investigation.

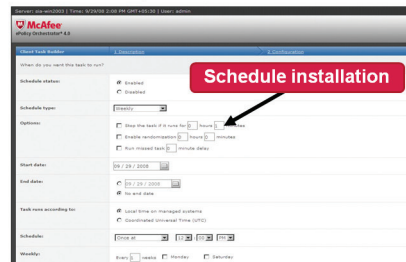
1. Manage deployments



2. Define tasks and policies



3. Schedule updates



4. Get asset coverage reports

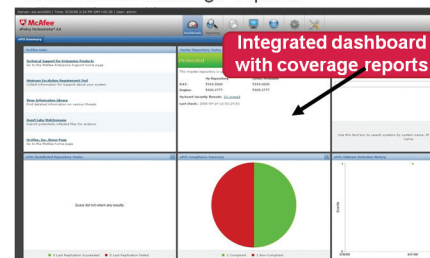


Figure 1. Deploying AccessData agents through McAfee ePO.

Recognized as an industry leader, AccessData delivers state-of-the-art computer forensic solutions. The integrated solution extends the capabilities of McAfee Total Protection for Endpoint—the industry’s most advanced endpoint security solution—while also lowering the total cost of ownership and delivering a more powerful security solution than is available from either vendor alone.

About AccessData

AccessData, a pioneer in the digital forensics industry, provides investigators with the tools to preview, search for, analyze, process and forensically preserve electronic evidence for the purposes of criminal investigations, internal investigations, incident response and eDiscovery. AccessData provides the technology and training that empower law enforcement, government agencies, and corporations to perform computer investigations with speed and efficiency.

About McAfee ePolicy Orchestrator (ePO) software

McAfee ePO software is the industry-leading security and compliance management platform. With its single agent and single-console architecture, ePO software provides intelligent protection that is automated and actionable, enabling organizations to reduce costs and improve threat protection and compliance.

