

Altiris Console Integration

CREDANT Mobile Guardian (CMG) Enterprise Edition provides centralized endpoint encryption management that mitigates risk and enables data security without interrupting business. Altiris is an easy to use systems management solution that reduces the total cost of ownership by allowing IT professionals to manage computing devices from virtually anywhere. By integrating the two solutions, customers can manage the entire lifecycle of their mobile devices and data security from the Altiris Console.

Why Integrate Altiris and CMG?

The increasing frequency of public disclosures around the loss or theft of personal information highlights a growing problem facing companies today: technology advances and security legislation have outpaced corporate data security. Companies are increasingly vulnerable to data loss, subsequent legal disclosure requirements, financial and legal liability and public relations headaches. Reports of data breaches damage customer relations, company brand, and ultimately share price.

“Data Breach” legislation enacted by the majority of US States requires companies to notify anyone if “their unprotected personal information was, or is reasonably believed to have been, acquired by an unauthorized person”. Companies encrypting endpoint data are considered to be compliant, and are not required to make any public notification in the event of a breach. To avoid public disclosure, they must be able to prove that any personal data on a lost or stolen device was encrypted. Detailed reports and device audits must demonstrate that encryption software was correctly installed, configured, and running on that device at the time of the loss.

For years, CREDANT customers have deployed the CREDANT Mobile Guardian client components via the Altiris Management Framework. Altiris customers have requested automated tools for deployment, management, and reporting from within the Altiris environment. Most were using Altiris for an array of tasks ranging from discovery and inventory to patch and software management. To satisfy customer demand, CREDANT ported its encryption management capabilities to Altiris. In particular, customers needed the ability to configure, deploy, manage, and report on encryption from within the Altiris Console. Responding to these requests, CREDANT and Altiris worked together to provide fully integrated deployment and management of CREDANT Mobile Guardian endpoint protection through the Altiris Console. Through this integration, customers have the ability to deploy, manage, and report on the state of their client encryption environment, from within the Altiris Console, thus easing the pain of compliance.

Altiris Console and Client Management Suite

Key features and Benefits:

- Secure management with role- and scope-based security
- Zero-touch OS deployment and migration
- Integrated hardware and software inventory with Web-based reporting
- Policy-based software management
- Automated patch management
- Software license compliance and harvesting
- Native integration with Microsoft Active Directory
- Centralized management of mixed hardware and OS environments

CREDANT Mobile Guardian Technical Overview

Policy-Based Intelligent Encryption™ for Full Data Protection

Unlike legacy encryption technologies, CREDANT's patent-pending Policy-based Intelligent Encryption delivers a multi-layered defense that results in full data protection. CMG supports critical business controls that ensure data is protected so companies are compliant with privacy and other regulations. Data files are encrypted and accessed transparently so there's no change in how users work and there's minimal impact on IT operations. CREDANT's on-the-fly process decrypts files as they are accessed, so data always remains encrypted on the drive and is only decrypted in memory while in use. CREDANT's defense-in-depth, Intelligent Encryption strategy extends compliance controls to mobile endpoints thus ensuring that corporate data on mobile endpoints and removable media is protected at all times.

CMG Architecture

CREDANT Mobile Guardian is composed of multiple components to enable installation in both small and large enterprise environments (Figure 1). Centrally administered by the CMG Enterprise Server infrastructure, CMG Shields enforce rich security and encryption policies to ensure data privacy and recovery for all protected data, even on removable media.

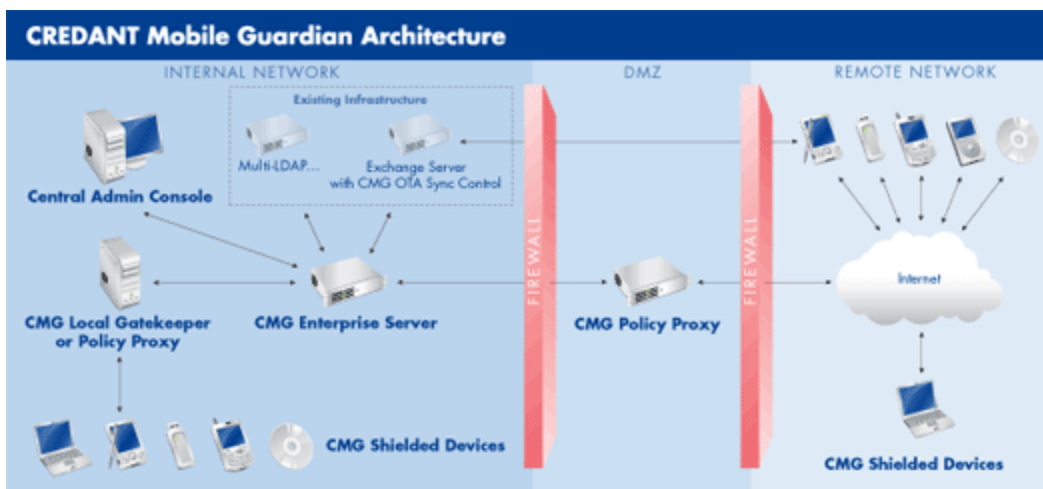


Figure 1. CREDANT Mobile Guardian Enterprise Infrastructure

CMG includes the following:

CMG Enterprise Server integrates with enterprise directories (e.g. Active Directory) to leverage existing users and groups for policy definition and reporting. The Server components provide a central, web-based interface for security policy definition and management, real-time mobile device inventory, and continuous reporting of mobile device security status for compliance.

Central Administrator Console provides a web based interface to the CMG Enterprise Server that can be accessed from inside or outside the corporate network. All communications are performed via SSL, and the Console GUI is accessed via any supported web browser. There is no management client to install.

CMG Policy Proxy resides in the corporate network or DMZ to provide secure and efficient distribution of policies and policy updates from the CMG Enterprise Server to the CMG Shields. It also collects device inventory and encryption status information that is passed to the CMG server for audit and reporting.

CMG Shield resides on laptops, desktops, handheld devices and external media to enforce mobile security policies even when the device is disconnected from the network. It enforces strong authentication, Policy-based Intelligent Encryption, and device and end-user controls.

CMG Local Gatekeeper resides on desktops and laptops to automatically detect, protect, and control mobile devices that synchronize locally to the corporate computer. It provides secure, distributed communications between CMG Handheld Shields and the CMG Enterprise Server for transparent delivery and management of policy and software updates.

Deploying CREDANT Mobile Guardian with Altiris

With this integration, the Altiris Framework can now be used to seamlessly deploy CMG client software to laptop and desktop computers. This allows the administrator to quickly identify systems that need encryption and deploy the CMG Shield to them, all from within a single management interface. Administrators can also use the Altiris Console to configure the CMG Shield installation package before deployment (Figure 2). This integration supports the full range of Windows Shields, including:

- CMG Enterprise Edition for Windows
- CMG External Media Edition for Windows
- CMG StandAlone Edition for Windows

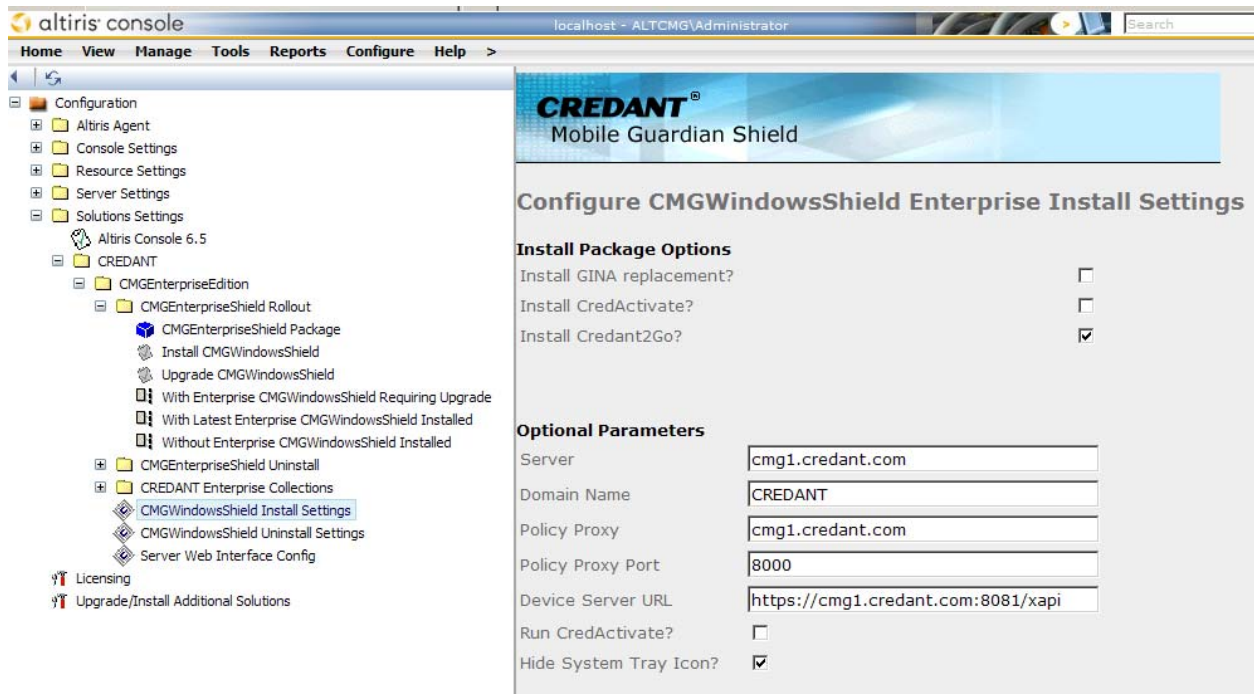


Figure 2. Configuring the CMG Shield Deployment Package

Once the installation package is configured, Shield deployment is as simple as choosing a collection of computers within the environment and either scheduling the installation for later or running the task immediately (Figure 3). The installation package is deployed using the Altiris agent at the endpoint.

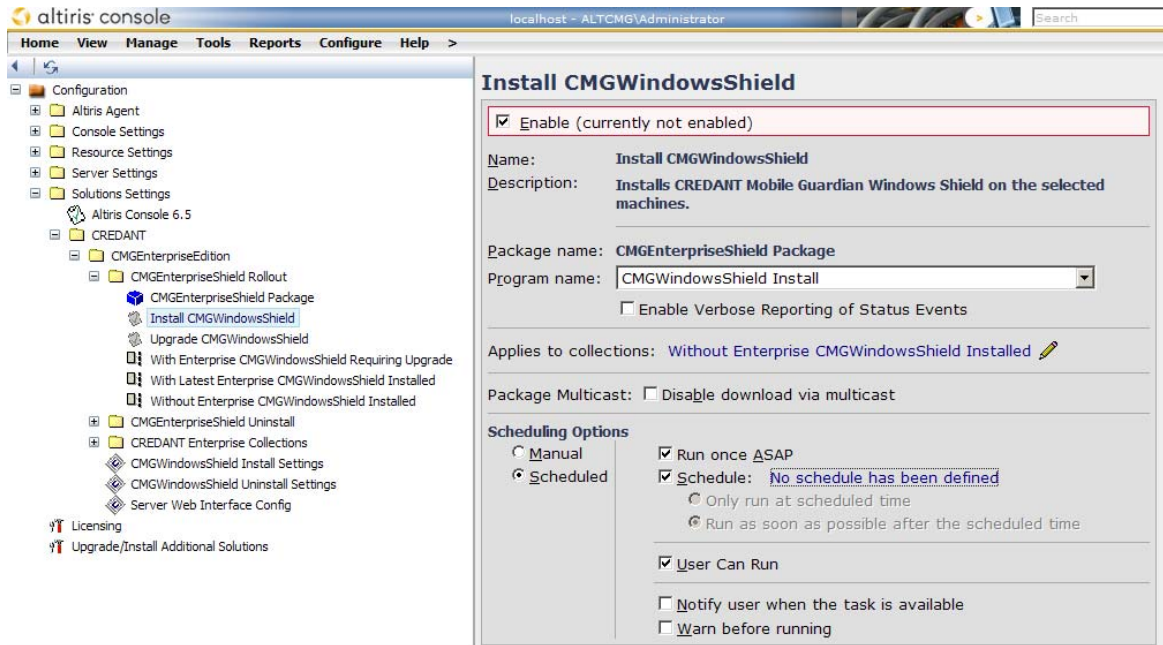


Figure 3. Administrator Interface to Define Shield Deployment

Once deployed, CMG Windows Shields are automatically displayed in the appropriate collection within the Altiris Console (Figure 4). This helps the administrator more easily identify which devices are protected by CREDANT Intelligent Encryption and which have not yet been protected.

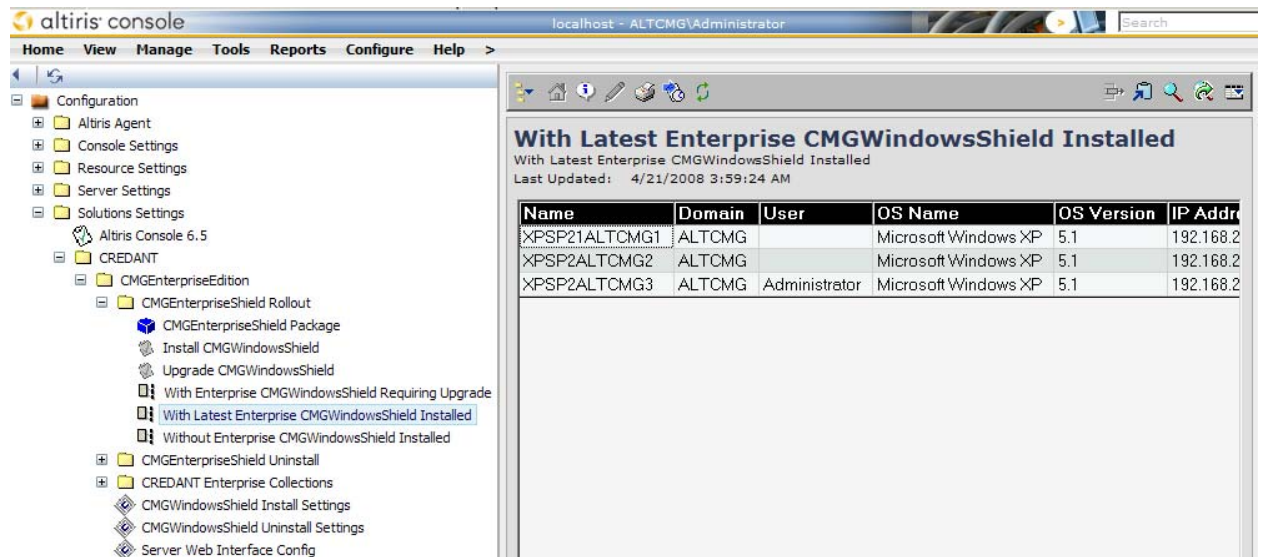


Figure 4. CMG Shields are Automatically Organized within the Altiris Console

Managing CREDANT Mobile Guardian with Altiris

There are a variety of options for managing CMG via Altiris. To further broaden the CMG management, customers can configure Altiris with the location of the CMG Server (Figure 5) and CREDANT Server Support Engine, which offers additional CMG reporting. Once this is complete, all CMG Management can be accessed from within the Altiris Console (Figure 6).

Full management of CREDANT protection includes details on policies applied to users, user groups, and devices. These policies can also be managed through the Altiris Console (Figure 7). Though CMG deployment via Altiris is only supported for Windows Computers, policy management via Altiris is provided for all device types, including Windows computers, Pocket PCs, Smartphones and Removable Media.

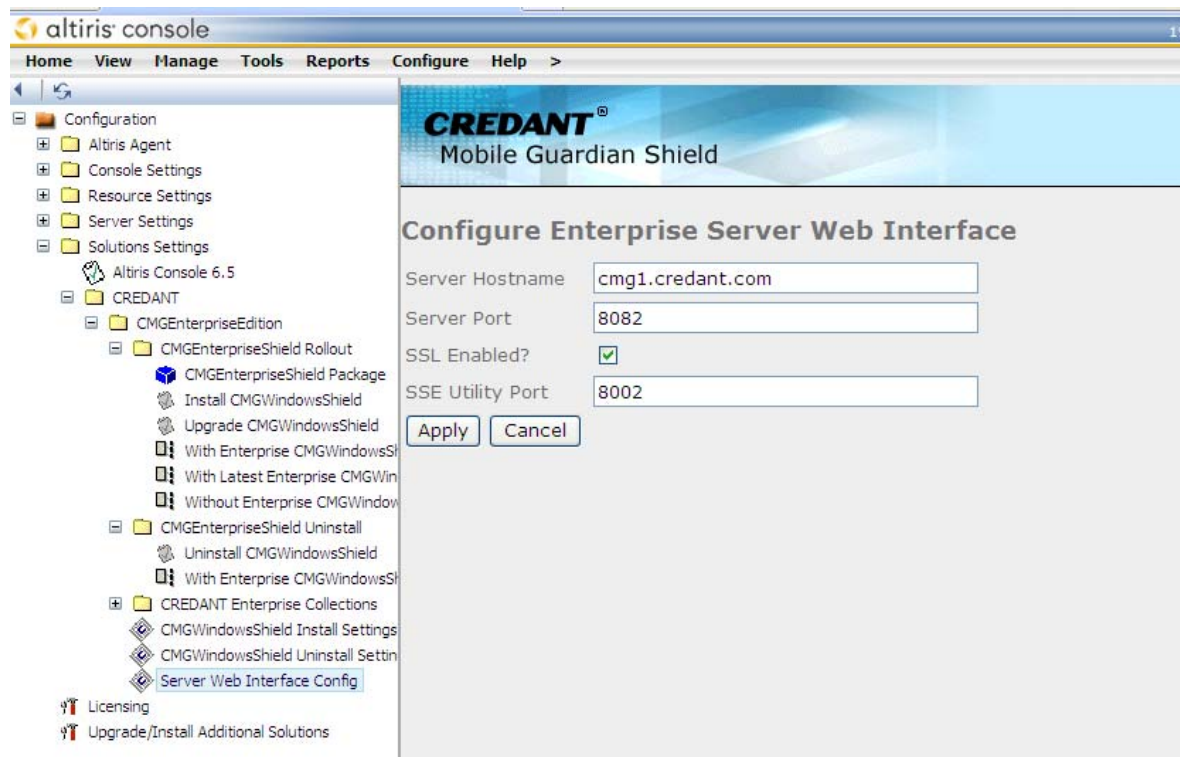


Figure 5. Configure CMG Server for Access via the Altiris Console

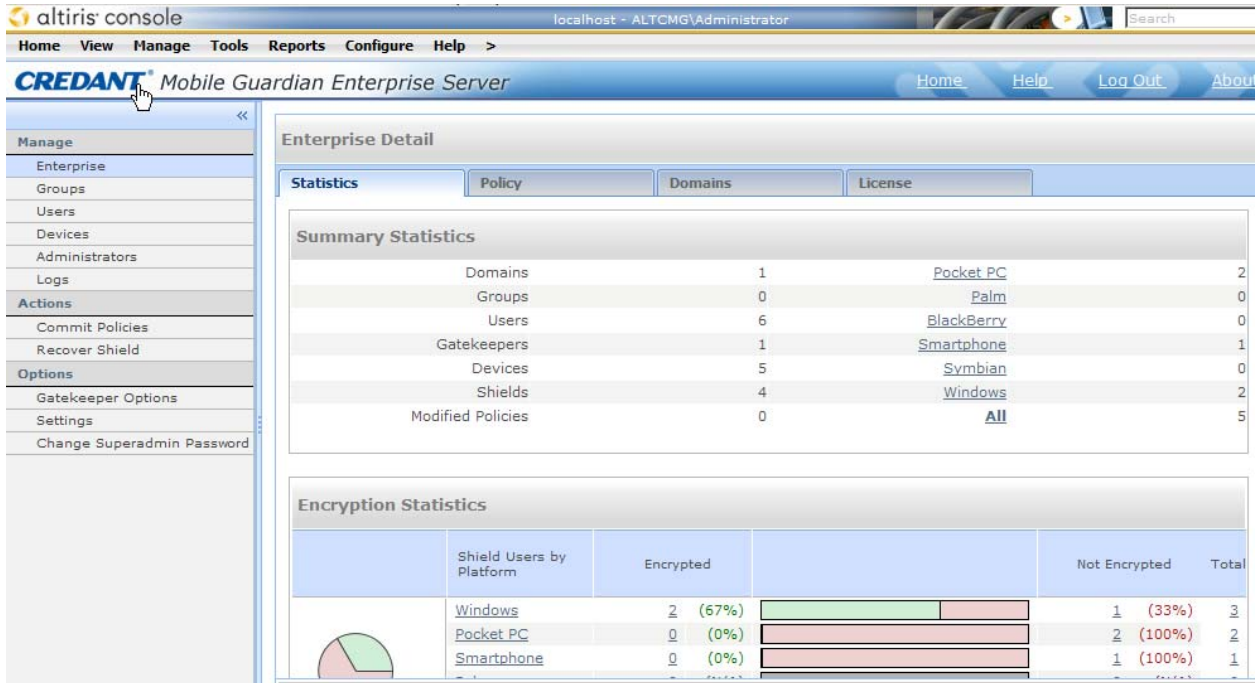


Figure 6. Accessing the CMG Console from Within the Altiris Console

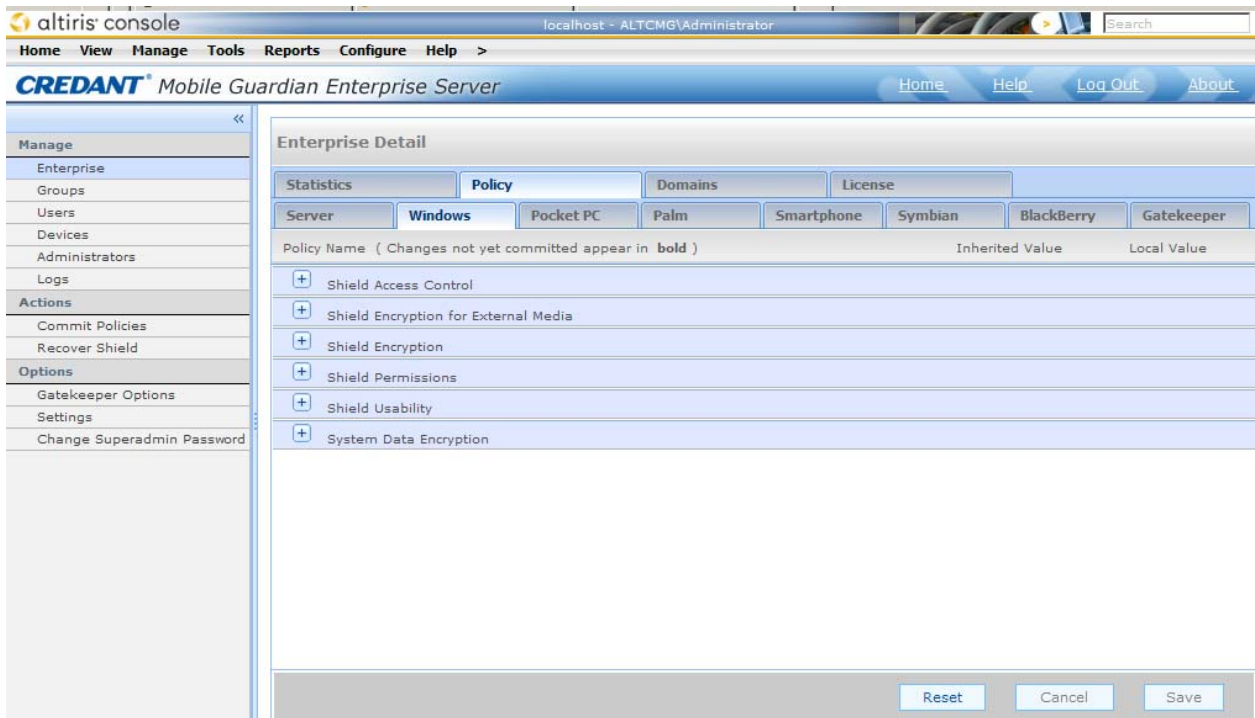


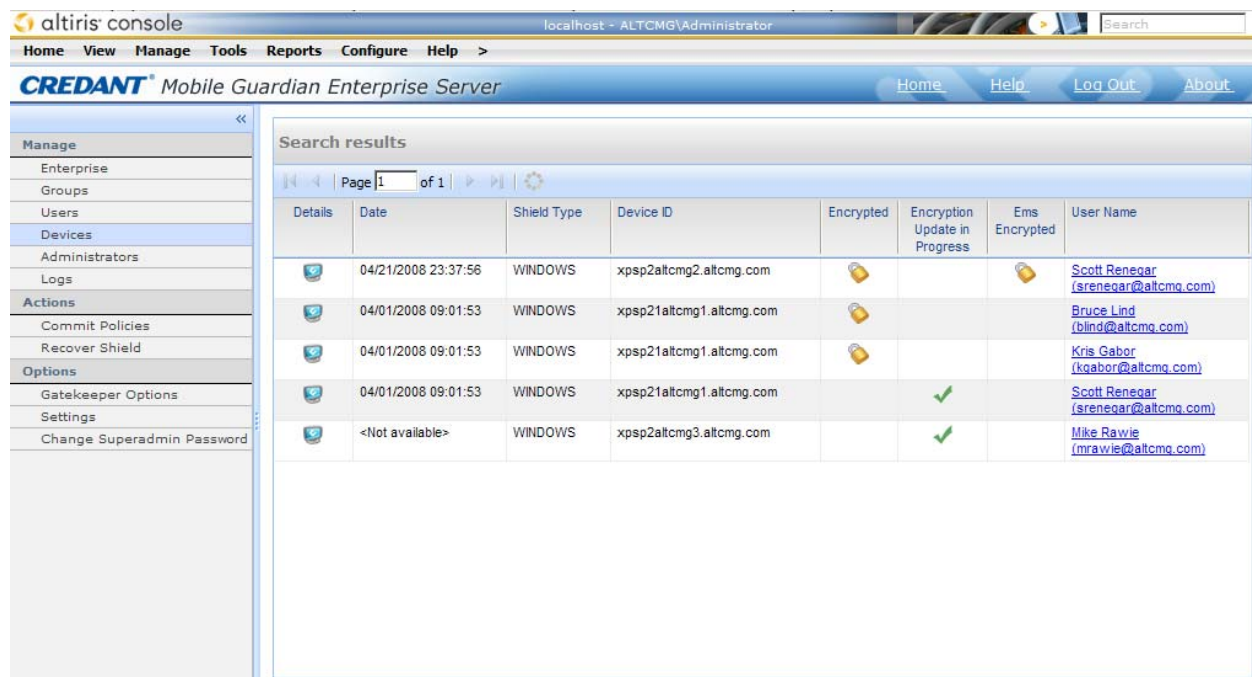
Figure 7. Configuring Device and User Encryption Policies from Within Altiris

Managing CREDANT Mobile Guardian with Altiris

Knowing that mobile device data is properly encrypted and protected is critical for proving compliance and avoiding breach notification. CREDANT Mobile Guardian was designed to provide organizations with up to date information regarding the state of data protection, even when a device has been lost or stolen. CREDANT's automatic inventory update process is the key to providing Administrators and Auditors with the data necessary to prove compliance. The CMG Server components work together to track and maintain mobile device inventory so organizations can see how many and what types of devices are connecting to their networks.

When a user logs on to a computer protected by the CMG Shield for Windows, inventory updates are sent to the CMG Enterprise Server for reporting. Inventory is also updated automatically for devices protected by the CMG Handheld Shields. Device inventory includes details about installed CMG components, protected users and the software, hardware and firmware installed. Other inventory detail includes the host name, IP address, last poll time, mobile user ID, device type, Operating System (OS) and OS version. Specific device inventory information is also collected, including available memory, total memory, and battery life (if applicable).

Through the CMG integration with the Altiris Console and the Altiris Agent, administrators can use the Altiris management interface to quickly identify devices that are running the CMG Shield, and report on the health and encryption status (Figure 8) for any protected device.



Details	Date	Shield Type	Device ID	Encrypted	Encryption Update in Progress	Ems Encrypted	User Name
	04/21/2008 23:37:56	WINDOWS	xpsp2altcmg2.altcmg.com				Scott Renegar (srenegar@altcmg.com)
	04/01/2008 09:01:53	WINDOWS	xpsp21altcmg1.altcmg.com				Bruce Lind (blind@altcmg.com)
	04/01/2008 09:01:53	WINDOWS	xpsp21altcmg1.altcmg.com				Kris Gabor (kgabor@altcmg.com)
	04/01/2008 09:01:53	WINDOWS	xpsp21altcmg1.altcmg.com				Scott Renegar (srenegar@altcmg.com)
	<Not available>	WINDOWS	xpsp2altcmg3.altcmg.com				Mike Rawie (mrawie@altcmg.com)

Figure 8. Encryption Status of CMG Protected Mobile Devices

Further integration allows CREDANT to utilize the Altiris Task Agent and Task Job processes to run more detailed encryption reports. Using CREDANT's WSScan utility in conjunction with the Altiris agent (Figure 9), administrators can produce highly detailed encryption status reports.

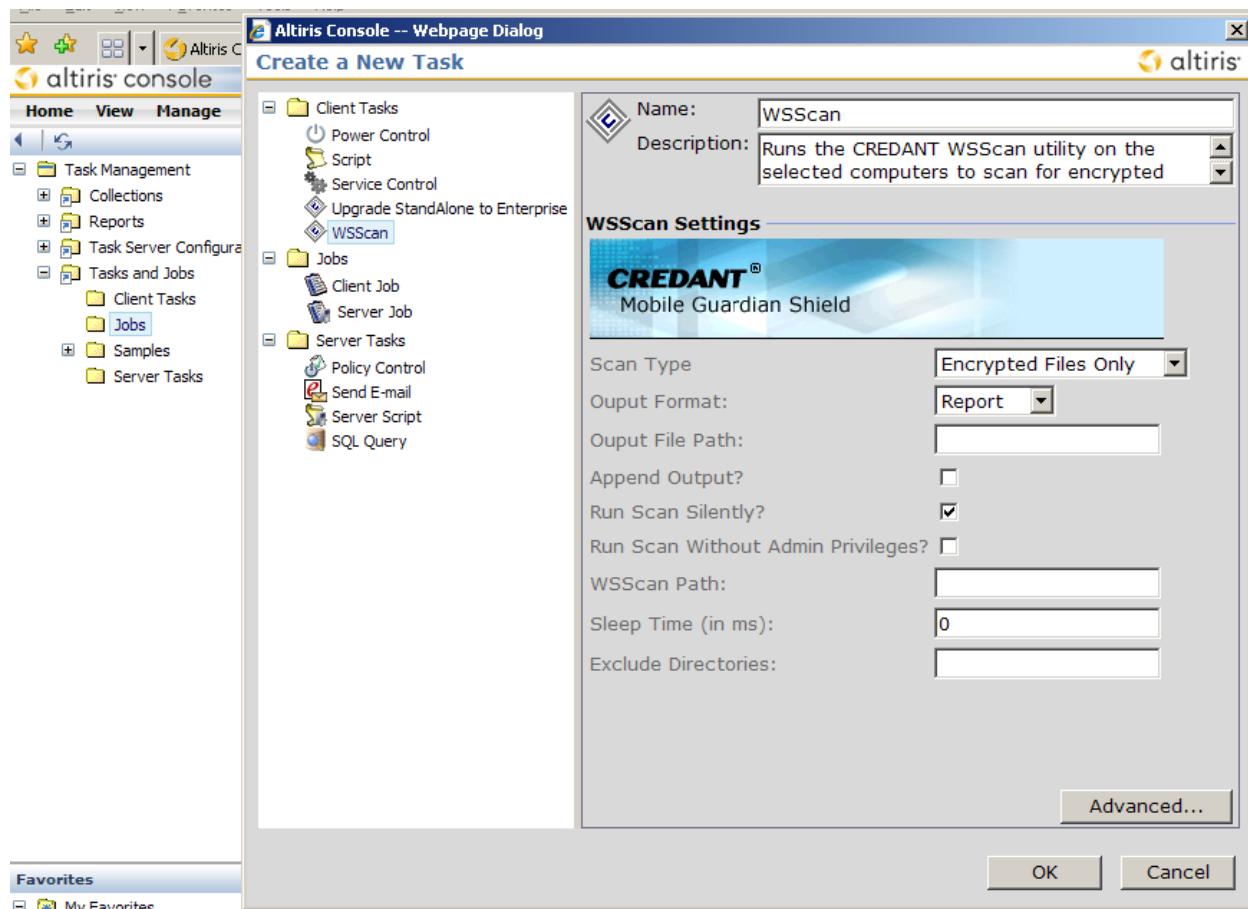


Figure 9. Administrator Configures an Altiris Task Job for the WSScan Utility

Summary

CREDANT Mobile Guardian Enterprise Edition supports today's sophisticated mobile enterprise environments with unique Intelligent Encryption while Altiris simplifies the IT process and reduces the cost of managing remote devices. The integration of CREDANT Mobile Guardian with the Altiris endpoint management platform allows IT administrators to use the Altiris console to manage encryption, audit, and deployment of CMG data protection on corporate endpoints. This integration supports the growing business imperative to protect sensitive data residing on computers, removable media and handheld devices while easing the IT burden. The combination of Altiris and CREDANT simplifies the control of critical data and devices by providing management and security from a single, enterprise console. The integration of the CREDANT and Altiris solutions automates the deployment and provisioning of encryption and allows companies to quickly locate unprotected corporate laptops and remediate that risk, which is critical for compliance.