



# MICROSOFT BITLOCKER ADMINISTRATION AND MONITORING (MBAM)



# MICROSOFT BITLOCKER ADMINISTRATION AND MONITORING (MBAM)

Microsoft BitLocker Administration and Monitoring™ (MBAM) provides a simplified administrative interface to BitLocker Drive Encryption™ (BDE). MBAM allows you to select BDE encryption policy options appropriate to your enterprise, monitor client compliance with those policies, generate reports on the encryption status of missing devices, and quickly provide BDE recovery keys to end users that have entered recovery mode. This hands-on demo will show you some of the management features available in MBAM. You will learn how to set enforcement and management policies, run compliance reports, and see how key recovery works using the Key Recovery Portal.

## Goals and Objectives

Brief goals overview

In this demo, you will:

- Explore changes to the MBAM features installation
- Review the installed elements of the MBAM solution
- Use Group Policy to provision the MBAM reporting and recovery components as well as enterprise BitLocker enforcement
- Review the MBAM client user experience
- Use MBAM reporting features
- Use the MBAM Key Recovery page to retrieve recovery key information

Estimated time to complete this demo: **60** minutes

## Virtual Machines used in this Demo

Virtual Machine Name: **MDOP-DC**

Computer Name: **DC**

Virtual Machine Name: **MDOP-Svr1**

Computer Name: **Svr1**

Virtual Machine Name: **MDOP-Client3**

Computer Name: **Client3**

## **Overview of the Microsoft BitLocker Administration and Monitoring (MBAM) Server Components**

Enterprise deployments of BitLocker Drive Encryption (BDE) are typically configured and managed using a combination of Group Policy, scripting, and custom reports. Consequently using BDE in an IT environment can become a complex IT administrative task to manage..

Microsoft BitLocker Administration and Monitoring (MBAM) 2.0 is a new solution developed for the configuration and management of BitLocker. MBAM provides tools for managing BitLocker device encryption (BDE), the secure storage of key recovery information, status reporting of BitLocker policy compliance, and IT support tools for recovery key recovery.

The following BitLocker Administration and Monitoring features represent the server infrastructure features for an MBAM server deployment: These features can be installed on a single server or distributed across multiple servers.

- Recovery and Hardware Database – The Recovery and Hardware Database stores the recovery key information and hardware profiles from each computer with the MBAM client agent installed.

- Compliance Status Database – The Compliance Status Database stores the current Bitlocker enforcement status for each MBAM client.

- Compliance and Audit Reports - The Compliance and Audit Reports provide a robust SQL Reporting Services based dashboard for Computer and User Compliance reports.

- Administration and Monitoring Server - MBAM installs an Administration and Monitoring web page, a central portal for compliance reporting and Bitlocker administration. Two services are installed by MBAM which must be configured in Group Policy to enable client monitoring and reporting: the MBAMComplianceStatusService and the MBAMRecoveryAndHardwareService.

- Self Service Key Recovery - Users can request their recovery key without the help desk.

- Configuration Manager Integration - Enables you to deploy MBAM with reduced infrastructure by enabling MBAM capability added to the existing Configuration Manager infrastructure.

In addition to the server related BitLocker Administration and Monitoring features, the server setup application includes a MBAM Group Policy template feature. The MBAM Group Policy template contains a superset of existing BitLocker Group Policies as well as the MBAM specific policies for configuring reporting and enforcement. This feature can be installed on any client able to run the Group Policy Management Console (GPMC) or Advanced Group Policy Management (AGPM).

The MBAM client component can be installed on any Windows 7 (Enterprise, Ultimate) or Windows 8 (Professional, Enterprise) computers with a Trusted Platform Module (TPM) v1.2 or v2.0. TPM 1.2 chips must be visible to the operating system and ownership must not have been taken while in the case of Windows 8 computers equipped with TPM v2 complete management is available by the operating system.

# 0 MICROSOFT BITLOCKER ADMINISTRATION AND MONITORING FEATURE INSTALLATION

In this exercise, we explore the installation options for MBAM 2.5.

Tasks	Detailed steps
1. Log on	<p>Log on to <b>DC</b> using the following credentials:</p> <p>User Name      <b>Administrator</b></p> <p>Password        <b>Password1</b></p> <p>Domain           <b>CONTOSO</b></p>
2. Install the MBAM server components	<p>Perform the following on <b>DC</b>.</p> <ol style="list-style-type: none"> <li>1. Open File Explorer and browse to <b>C:\Labfiles</b> and double-click <b>MbamServerSetup.exe</b></li> <li>2. On the welcome page, click <b>Next</b>.</li> <li>3. Accept the UELA and click <b>Next</b>.</li> <li>4. Select <b>Do not join the program at this time</b> and then click <b>Next</b>.</li> <li>5. Click <b>Install</b> to begin the installation.</li> </ol> <p>You can now preinstall the MBAM components on each server what will run MBAM services. This makes deployment of the environment easier for scenarios like automated installations using powershell.</p> <ol style="list-style-type: none"> <li>6. When the installation is complete, click <b>Finish</b>.</li> </ol>
3. Add new features	<ol style="list-style-type: none"> <li>1. On the BitLocker Administrations and Monitoring wizard, click <b>Add New Features</b>.</li> <li>2. On the Select Features to Add page, select the following options and then click <b>Next</b>. <ul style="list-style-type: none"> <li>▪ <b>Compliance and Audit Database</b></li> <li>▪ <b>Recovery Database</b></li> <li>▪ <b>Administration and Monitoring Website</b></li> <li>▪ <b>Self-Service Portal</b></li> </ul> </li> <li>3. When the prerequisite checks are completed, click <b>Next</b>.</li> <li>4. On the Configure Database page, under <b>Compliance and Audit Database</b>, fill in the following fields. <ul style="list-style-type: none"> <li>▪ SQL Server Name: <b>svr1</b></li> <li>▪ Read/write access domain user or group: <b>contoso\administrator</b></li> <li>▪ Read-only access domain user or group: <b>contoso\administrator</b></li> </ul> </li> <li>5. Under Recovery Database, fill in the following fields and then click <b>Next</b>. <ul style="list-style-type: none"> <li>▪ SQL Server Name: <b>svr1</b></li> <li>▪ Read/write access domain user or group: <b>contoso\administrator</b></li> </ul> </li> </ol> <p>MBAM 2.5 now supports high availability configurations on Windows Server, IIS, and SQL Server. MBAM supports load balancing of its web components using software or hardware based load balancers and its databases can now be deployed to SQL Server failover clusters.</p>

6. On the Configure Web Applications page, under Configuration for all Web Applications, click **Browse** next to Security Certificate, select the first certificate and click **OK**.
7. For Web service application pool domain account, enter a username of **contoso\administrator** and password of **Password1**.
8. Under Administration and Monitoring Website, fill in the following fields and then click **Next**.
  - Advanced Helpdesk role domain group: **contoso\mbamadvancedhelpdesk**
  - Helpdesk role domain group: **contoso\mbamhelpdesk**
  - Reporting role domain group: Contoso\domain admins
  - SQL Server Reporting Services URL: **Https://svr1.contoso.com/reportserver**
9. On the Summary page, click **Export Powershell script** and save it to the Desktop.
10. Click **Cancel** on the Microsoft BitLocker Administration and Monitoring wizard.

The services have already been installed and configured to save on time.

11. Click **Yes** on the confirmation prompt.
12. On the desktop, double-click Add-Mbamfeatures.ps1.
13. Explore the PowerShell commands and close the file.

# 1 MICROSOFT BITLOCKER ADMINISTRATION AND MONITORING FEATURES

In this exercise, we will look at some of the installed features and requirements for the Microsoft BitLocker Administration and Monitoring (MBAM) solution.

Tasks	Detailed steps						
4. Log on	<p>Log on to <b>SVR1</b> using the following credentials:</p> <table border="0"> <tr> <td>User Name</td> <td><b>Contoso\Administrator</b></td> </tr> <tr> <td>Password</td> <td><b>Password1</b></td> </tr> <tr> <td>Domain</td> <td><b>CONTOSO</b></td> </tr> </table>	User Name	<b>Contoso\Administrator</b>	Password	<b>Password1</b>	Domain	<b>CONTOSO</b>
User Name	<b>Contoso\Administrator</b>						
Password	<b>Password1</b>						
Domain	<b>CONTOSO</b>						
5. Review the installed database features	<p>Perform the following on <b>SVR1</b>.</p> <ol style="list-style-type: none"> <li>1. Mouse to the upper right corner to open the <b>Charms</b> bar. Select the <b>Start</b> charm.</li> <li>2. On the top left side of the screen, launch <b>SQL Server Management Studio</b>.</li> <li>3. On the Connect to SQL dialog, click <b>Connect</b>.</li> <li>4. In the Object Explorer, expand <b>SVR1   Databases</b>.</li> </ol> <p>The two database components configured when installing Microsoft BitLocker Administration and Monitoring (MBAM) are the Compliance Status Database and the Recovery and Hardware Database.</p> <p><i>MBAM Compliance Status Database</i> – The MBAM Compliance Status Database stores the current Bitlocker enforcement status for each MBAM client</p> <p><i>MBAM Recovery and Hardware Database</i> – The MBAM Recovery and Hardware stores the recovery key information and hardware profiles from each computer with the MBAM client agent installed.</p> <p>The Microsoft BitLocker Administration and Monitoring (MBAM) database and reporting features require Microsoft SQL Server R2 or Microsoft SQL Server 2008 Database and Reporting Services on either the Standard, Developer, Enterprise or Datacenter editions.</p> <ol style="list-style-type: none"> <li>5. In the Object Explorer, expand <b>SVR1   Security   Logins</b>.</li> <li>6. Under the Logins node, take note of the following access accounts:  <b>SVR1\MBAM Compliance Auditing DB Access</b>  <b>SVR1\MBAM Recovery and Hardware DB Access</b></li> </ol> <p>MBAM installs two user groups with access to the Compliance Status and Recovery and Hardware databases.</p> <ol style="list-style-type: none"> <li>7. Close SQL Server Management Studio.</li> <li>8. Mouse to the upper right corner to open the <b>Charms</b> bar, select <b>Start</b>.</li> <li>9. On the top left side, click the <b>Internet Information Services (IIS) Manager</b> tile.</li> <li>10. In <b>IIS Manager</b>, expand <b>SVR1 &gt; Sites &gt; Microsoft BitLocker Administration</b>.</li> <li>11. The MBAM server components are all IIS based. Examine the various back-end service applications and take note of the <b>HelpDesk</b> and</li> </ol>						

	<p><b>SelfService</b> applications. We will examine the use of these sites later in the demo.</p>
--	---

12. Close **IIS Manager**.

## 2 PROVISIONING ADMINISTRATION AND MONITORING POLICY

Microsoft BitLocker Administration and Monitoring (MBAM) provides a Group Policy template that helps you configure the enterprise BitLocker enforcement settings as well as the typical enterprise BitLocker enforcement policies.

In this exercise we will configure the key recovery and status reporting endpoints, as well as configure a BitLocker enforcement policy for a department organizational unit.

Tasks	Detailed steps
1. Explore the backend and status reporting policies	<p>Perform the following on <b>DC1</b>.</p> <ol style="list-style-type: none"> <li>1. Mouse to the upper right corner to open the <b>Charms</b> bar and select the <b>Start</b> charm.</li> <li>2. On the left hand side select <b>Group Policy Management</b>.</li> <li>3. In the console tree, right-click <b>MDOP</b> and click <b>Edit</b>.</li> <li>4. In the Group Policy Management Editor, expand <b>Computer Configuration   Policies   Administrative Templates   Windows Components</b> and click <b>MDOP MBAM (BitLocker Management)</b>.</li> </ol> <p>The MDOP MBAM (Bitlocker Management) node represents a superset of the existing BitLocker Drive Encryption policies available in the Windows Server 2008 and Windows Server 2008 R2 schema, as well as the MBAM recovery and reporting policies. It is suggested that when implementing MBAM, administrators exclusively use the MDOP MBAM (BitLocker Management) node for all BitLocker policy.</p> <ol style="list-style-type: none"> <li>5. In the console tree, expand <b>MDOP MBAM (BitLocker Management)</b> and click <b>Client Management</b>.</li> <li>6. In the details pane, double-click <b>Configure MBAM services</b>.</li> <li>7. In the Configure MBAM services window, note the available options.</li> </ol> <p>The MBAM Status reporting service endpoint value is only used when using MBAM in a stand-alone configuration. An error event will be generated on the MBAM client machine if the status reporting service endpoint value is defined when MBAM is deployed in SCCM integrated mode. In this demo, we are using SCCM. As such, do not configure the path below. It is provided as a reference. <a href="http://SVR1.contoso.com:2443/MBAMComplianceStatusService/StatusReportingService.svc">http://SVR1.contoso.com:2443/MBAMComplianceStatusService/StatusReportingService.svc</a></p> <ol style="list-style-type: none"> <li>8. Click <b>Next Setting</b>.</li> <li>9. On the <b>Configure user exemption policy</b>, click to select the <b>Enabled</b> radio button and configure the following options:            Select the method of contacting users with instructions: <b>Provide an email address</b>            Enter the appropriate e-mail address: <b>support@contoso.com</b></li> <li>10. Click <b>OK</b>.</li> <li>11. Close Group Policy Management Editor.</li> </ol>
2. Configure BitLocker enforcement for Marketing Department	<ol style="list-style-type: none"> <li>1. In the Group Policy Management Console, right-click the <b>Marketing OU</b> and click <b>Create a GPO in this domain, and Link it here...</b></li> <li>2. In the New GPO dialog, enter a name of <b>Marketing Bitlocker Enforcement</b> and click <b>OK</b>.</li> </ol>

3. In the console tree, expand the **Marketing** OU, right-click **Marketing Bitlocker Enforcement** and click **Edit**.
4. In the Group Policy Management Editor, expand **Computer Configuration | Policies | Administrative Templates | Windows Components | MDOP MBAM (BitLocker Management)**.
5. In the console tree, click **Operating System Drive**.
6. In the details pane, double-click **Operating system drive encryption settings**.
7. Click to select the **Enabled** radio button and configure the following values:  
Select protector for operating system drive: **TPM and PIN**  
Allow enhanced PINs for startup: Unchecked (default)  
Configure minimum PIN length for startup: **8**
8. Click **OK**.
9. In the console tree, click **Removable Drive**.
10. In the details pane, double-click **Control use of BitLocker on removable drives**.
11. Click to select the **Enabled** radio button.
12. Click **Next Setting**.
13. On the Deny write access to removable drives not protected by BitLocker page, click to select the **Enabled** radio button.
14. Click **OK**.
15. Close Group Policy Management Editor.
16. Close Group Policy Management console.

### 3 CLIENT AGENT USER EXPERIENCE -FULL

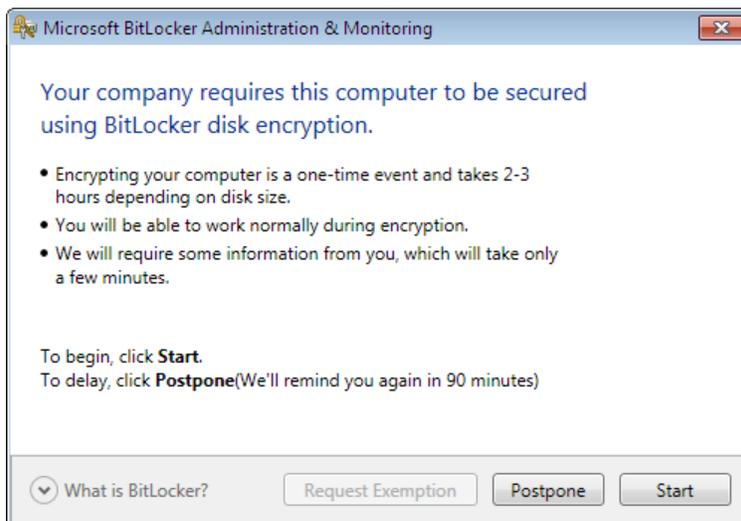
The Microsoft BitLocker Administration and Monitoring (MBAM) client agent can be installed at deployment or advertised using either MDT 2012 Update 1, System Center Configuration Manager (2007, 2012), Group Policy, or any third party software distribution tool you prefer. The client agent has a service component that will automatically start and report according to policies set in Group Policy. Additionally, the MBAM client has a user friendly interface that will prompt for BitLocker enforcement according to corporate policy.

In this exercise we will preview the MBAM client experience.

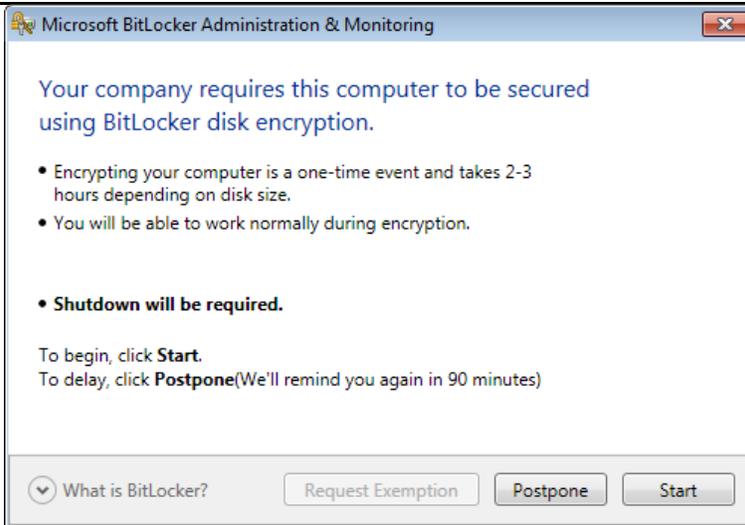
The following steps are informational only, due to the fact the virtual machines do not support Bitlocker encryption. Click-through steps will continue in in exercise 5.

#### Detailed steps

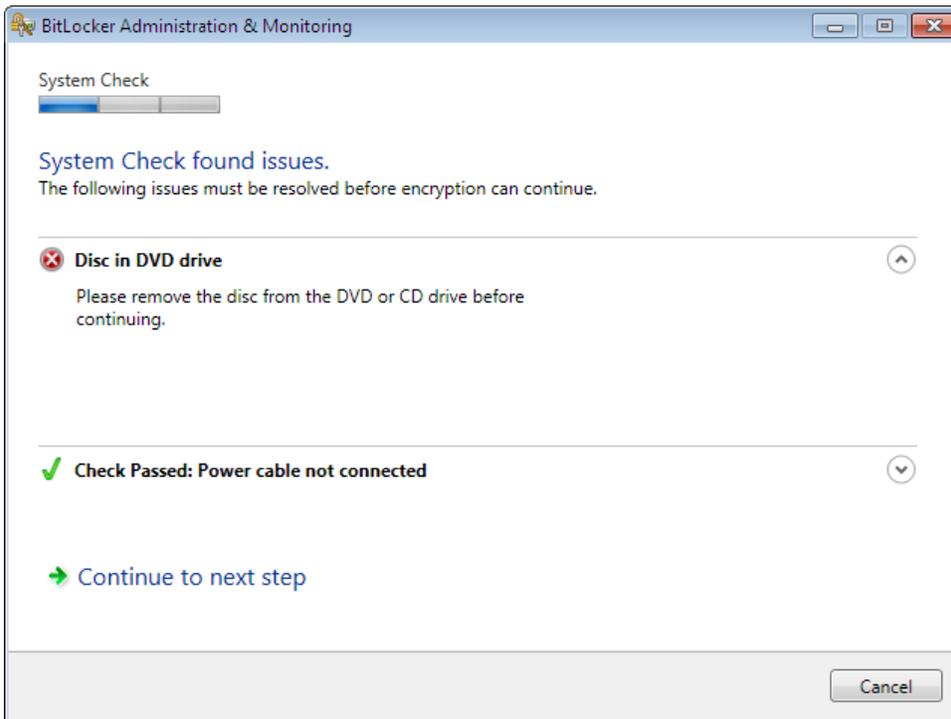
1. When a client logs on to a domain joined machine running the MBAM client agent and policies, the user will see the following wizard if their machine is not secured with BitLocker:



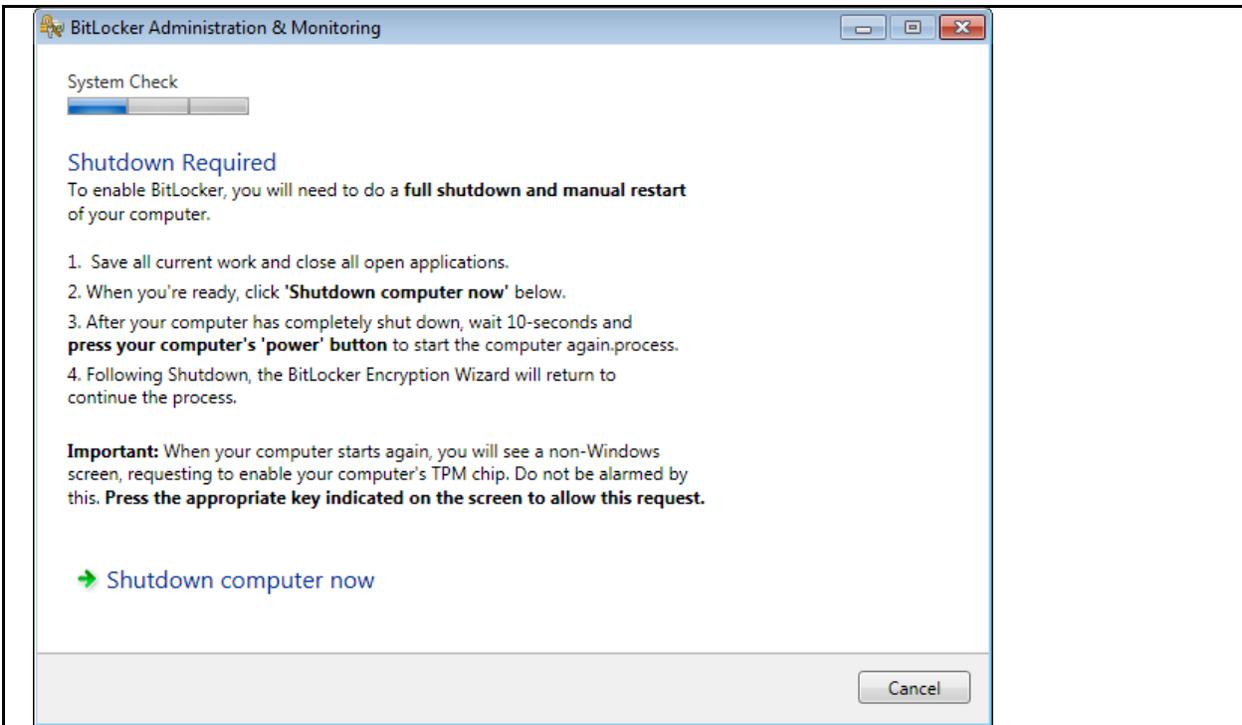
2. If the TPM needs to be cleared and ownership taken, the wizard will note that a shutdown will be required before the encryption process can begin.



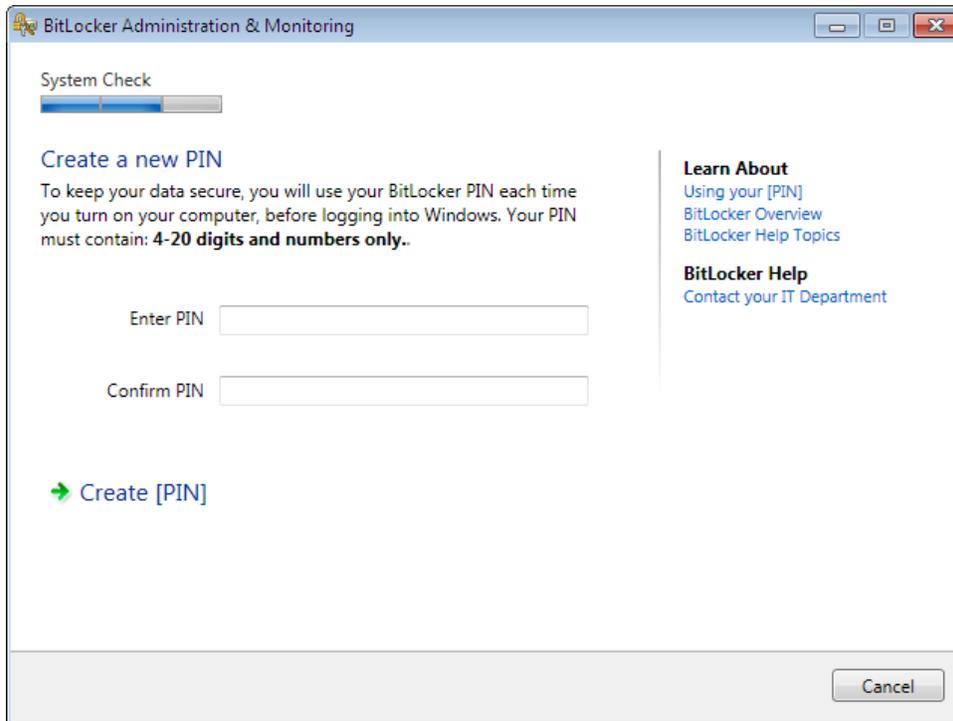
3. After the user clicks Start, the wizard will perform a System Check to look for any issues that will conflict with the encryption process.



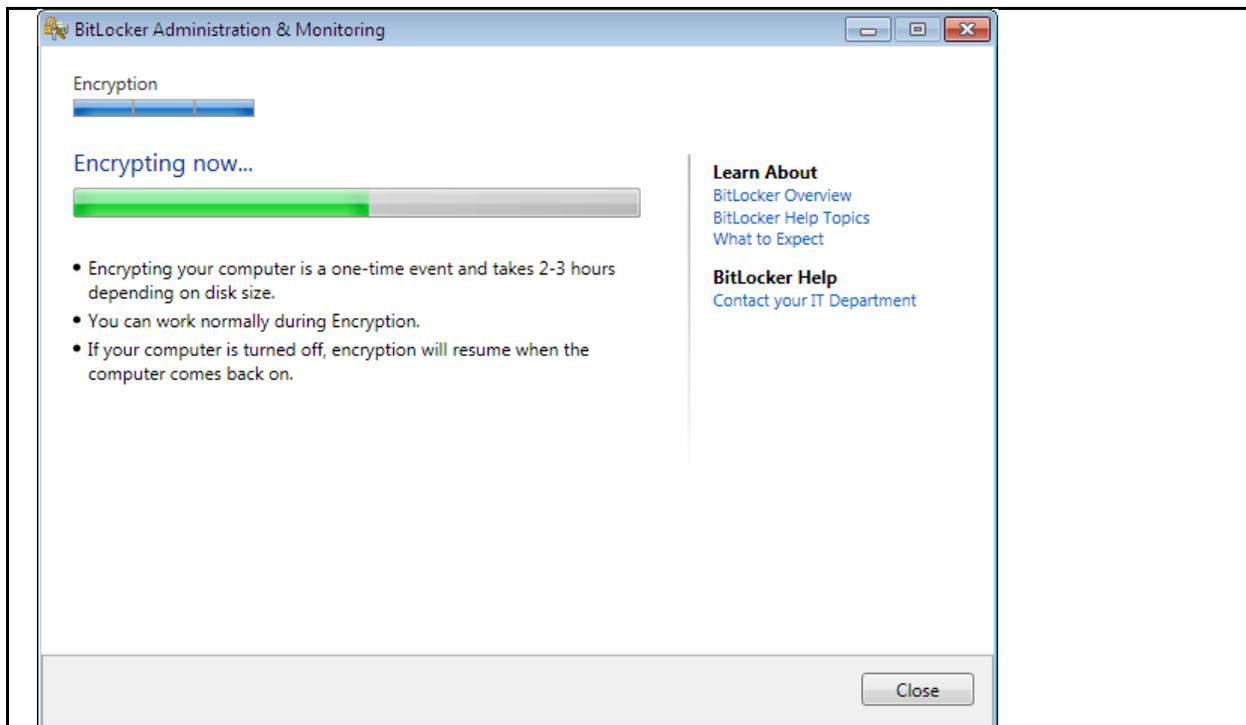
4. When the TPM needs to be cleared and ownership taken, the wizard will prompt for a full shutdown and manual restart of the computer. After TPM ownership has been taken and the reboot performed, the wizard will continue with the encryption process.



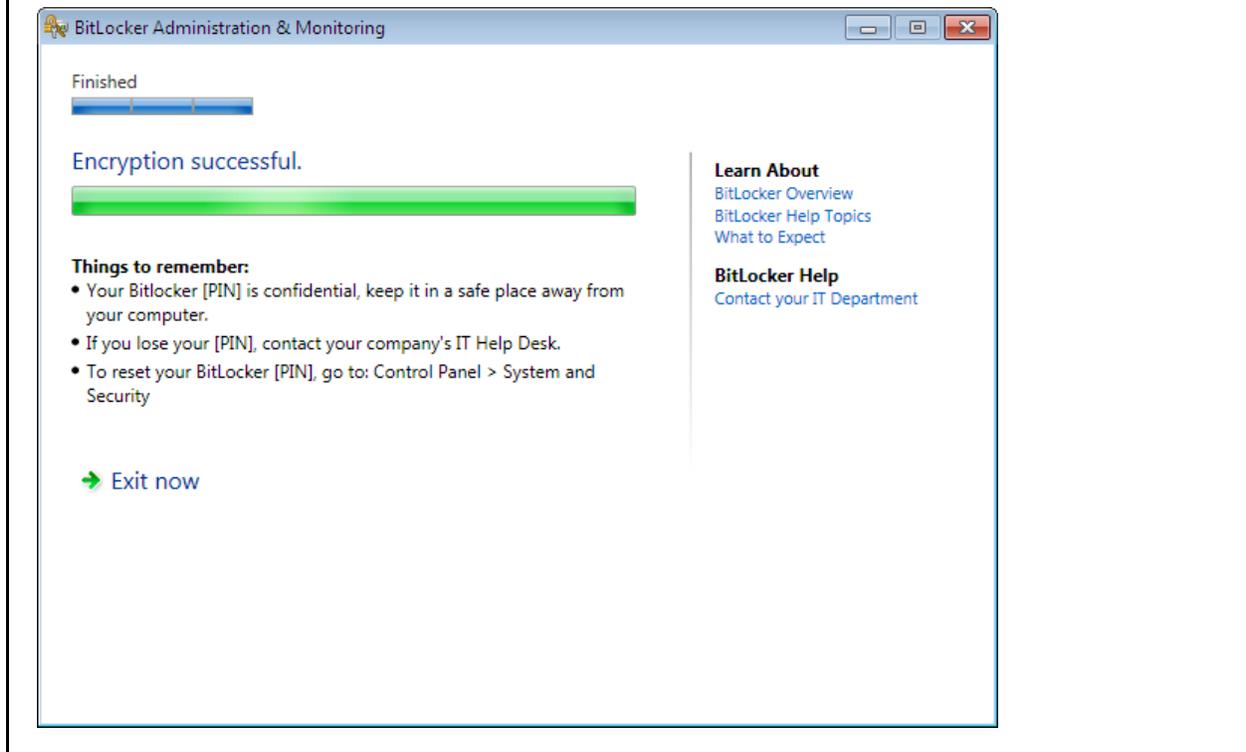
5. If there are no issues or TPM configuration needed, the wizard will continue directly to the Create a new PIN page (if the policy is configured to require a PIN), where the user will be prompted to create a PIN according to the length specifications set in Group Policy:



6. If the PIN entered meets the policy requirements, the wizard will begin the encryption of the policy specified drive:



7. The dialog can be closed while encryption takes place and users will be able to work normally during the encryption process, otherwise the wizard will display a success status at the end of the encryption process:



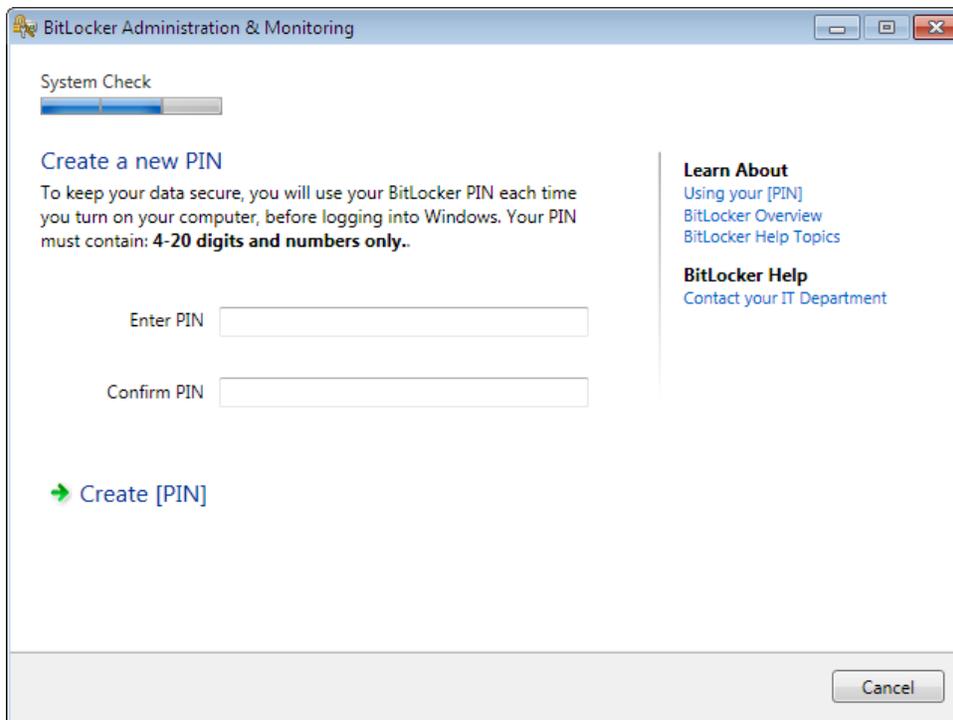
## 4 BITLOCKER CLIENT AGENT USER EXPERIENCE –PIN ONLY

In this exercise we will preview the MBAM client experience for a scenario where a new machine has been imaged and encrypted by IT using the MBAM client. While the device has been encrypted before the user receives it IT wants the user to add additional protection in the form of a custom PIN. The pre-boot PIN will prevent the PC from booting before PIN authentication. In this case the user will add the custom PIN after they log onto the device for the first time.

The following steps are informational only, due to the fact the virtual machines do not support Bitlocker encryption. Click-through steps will continue in exercise 5.

### Detailed steps

8. When a user logs on to a domain joined machine that has already been encrypted with Bitlocker and the MBAM client agent is deployed, the user will see the following wizard requiring them to create their PIN:



The screenshot shows a window titled "BitLocker Administration & Monitoring". At the top, there is a "System Check" progress bar. Below that, the main heading is "Create a new PIN". The text reads: "To keep your data secure, you will use your BitLocker PIN each time you turn on your computer, before logging into Windows. Your PIN must contain: 4-20 digits and numbers only..". There are two input fields: "Enter PIN" and "Confirm PIN". To the right of the input fields, there is a "Learn About" section with links for "Using your [PIN]", "BitLocker Overview", and "BitLocker Help Topics". Below that is a "BitLocker Help" section with a link for "Contact your IT Department". At the bottom left, there is a green arrow icon followed by the text "Create [PIN]". At the bottom right, there is a "Cancel" button.

9. If the PIN entered meets the policy requirements, the wizard is complete.

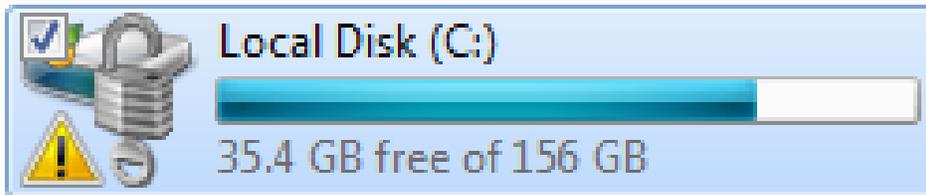
## 5 CLIENT AGENT USER EXPERIENCE –RESUMING BITLOCKER

Another scenario that MBAM can help with is when a user travels to a region where laws prohibit the use of TPM protection with Bitlocker or when an administrator needs to perform a BIOS update.

The following steps are informational only, due to the fact the virtual machines do not support Bitlocker encryption. Click-through steps will continue in exercise 5.

### Detailed steps

1. The user or Administrator suspends Bitlocker encryption resulting in the Bitlocker drive icon changing from gold to gray as in the image below:



2. It is common that on occasion the user or administrator might forget to re-enable Bitlocker encryption after returning or completing the BIOS update leaving the drive in a vulnerable, unprotected state.
3. To address this scenario, Windows 8 automatically resumes protection on restart, Windows will resume encryption when the machine is back on the corporate network MBAM can detect that Bitlocker is suspended and automatically resume Bitlocker encryption:



This feature further improves compliance with corporate standards on Bitlocker protection.

## 6 COMPLIANCE AND AUDIT REPORTING

Microsoft BitLocker Administration and Monitoring (MBAM) allows IT administrators to track the status of BitLocker on corporate desktops and laptops, as well as generate compliance reports for security administration. The reporting can be done on a computer level, useful particularly in the case of lost or stolen computers, or at the organizational level, in order to check corporate wide compliance.

System Center Configuration Manager (SCCM) integration makes the collection and reporting of all this data easy.

In this exercise we will view a variety of reports and filter data available through the MBAM reports available from SCCM.

Tasks	Detailed steps
1. View the SCCM MBAM Enterprise Compliance Dashboard	<p>Perform the following on <b>SVR1</b>.</p> <p>The Enterprise Compliance Dashboard within SCCM provides a central report providing a broad view of the overall MBAM footprint.</p> <p>The other MBAM reports such as the <b>Computer Compliance</b> and <b>Enterprise Compliance</b> reports can be accessed by clicking on specific resources within the Enterprise Compliance Dashboard.</p> <ol style="list-style-type: none"> <li>1. From the taskbar launch the <b>System Center Configuration Manager</b> console (icon furthest on the right).</li> <li>2. In the lower, left-hand pane select <b>Monitoring</b>.</li> <li>3. In the upper, right-hand tree expand <b>Reporting &gt; MBAM</b> and select <b>en-US</b>.</li> <li>4. In the details pane, right-click <b>Bitlocker Enterprise Compliance Dashboard</b> and select <b>Run</b>.</li> </ol> <p>Notice a series of graphs and charts displaying the overall Bitlocker status on machines throughout the enterprise.</p> <ol style="list-style-type: none"> <li>5. Examine the different graphs provided.</li> </ol>
2. View an Enterprise Compliance report.	<ol style="list-style-type: none"> <li>1. In the <b>Compliance Status Distribution</b> pie chart click the <b>green pie slice</b> to more closely examine the machines that have reported as <b>compliant</b>.</li> <li>2. The <b>Enterprise Compliance Report</b> is displayed. Examine the data in this report.</li> </ol> <p>This Enterprise Compliance Report is showing details about the <b>150</b> machines in the inventory that have reported as <b>Compliant</b> per our selection in the dashboard.</p> <p>Data shown includes <b>Computer Names, Domain Name, Compliance and Exemptions status the Users</b>.</p>
3. View a Computer Compliance Report	<ol style="list-style-type: none"> <li>1. In the <b>Enterprise Compliance Report</b> click the first computer in the list, machine <b>MBAMClient16777445</b> to generate a <b>Computer Compliance Report</b> so we can dig deeper into the makeup of that computer.</li> <li>2. The <b>Computer Compliance Report</b> is displayed. Examine the data in this report.</li> </ol>

This Computer Compliance Report is showing details about a specific machine we have selected from the Enterprise Compliance Report.

Data shown includes the **Domain Name, Computer Type (portable/non-portable), the Operating system, Compliance status, Exemption status, Cypher Strength, Encryption policies** that are in place, **Make and Model, Device users** and details about the computers **drives** and **TPM makeup and status.**

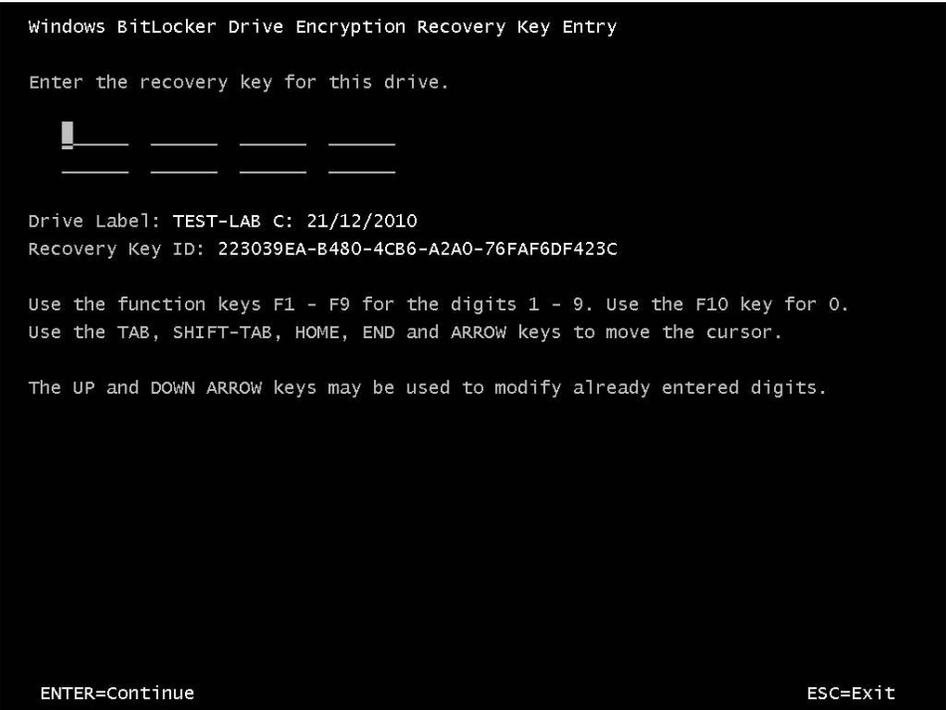
3. Close the **Computer Compliance Report.**
4. Back in the MBAM Reports details pane on the SCCM console, **notice** that you can also run each of those reports individually and separate from the dashboard if you choose.
5. Close the ConfigMgr console.

## 7 KEY RECOVERY USING THE SELF SERVICE PORTAL

A primary feature of the Microsoft BitLocker Administration and Monitoring solution is Key Recovery. This feature is useful for cases where the user has lost a PIN or Password for a drive.

MBAM provides a User Self Service Portal allowing users to recover their own Recovery Key without generating the additional work for the Help Desk staff.

In this exercise, we will look at the scenario of a lost PIN leading to a drive lock-out and prompt for a recovery password for the drive. The user will use the Self Service Portal to obtain the recovery key.

Tasks	Detailed steps
	<p>1. When a user has lost their PIN, they will enter recovery mode and be prompted by BitLocker to enter a recovery password in order to regain access to the encrypted drive.</p>  <p>Without MBAM, typically a user will have to consult with the help desk who will in turn need to escalate to someone with access to the key recovery data stored in Active Directory (a feature that must be enabled in Group Policy).</p>
2. Review User Self Service Portal key recovery method	<p>Perform the following on <b>SVR1</b>.</p> <ol style="list-style-type: none"><li>To reduce the likelihood of typos in this section, perform the following steps to copy the Bitlocker code used in this section to the clipboard:<ol style="list-style-type: none"><li>Open <b>Windows Explorer</b> and browse to <b>C:\Labfiles</b>.</li><li>Double-click <b>MBAMkeys.txt</b> to open the file in notepad.</li><li>Copy the entire hexadecimal code next to <b>KeyId 1</b> to the <b>clipboard</b>.</li><li><b>Close</b> notepad.</li><li><b>Close</b> Windows Explorer.</li></ol></li><li>On the <b>Desktop</b>, double-click the <b>MBAM Self Service</b> IE Link.</li></ol>

**Maximize** the IE window. The first page to appear is a **Notice**. Notice that the text of this notice can be changed by editing the .txt file shown in the body of the default notice.

3. Scroll to the bottom of the page, check the box labeled **I have read and understand the above notice** and click **Continue**.

The **User Self Service** portal uses an easy to follow 3-step format to reduce complexity for the end user.

4. Right-click within the **Recovery KeyId** field and select **paste** to paste in the key copied earlier.
5. Click the **Reason** pull-down menu and select **Lost PIN/Passphrase**.
6. Click **Get Key**.
7. Scroll down in the page, notice that the 48 digit Bitlocker Recovery Key has been presented to the user in the step 2 box.
8. The user is also provided instructions for how to manage their BitLocker PIN in the step 3 box.
9. Close **Internet Explorer**.

## 8 KEY RECOVERY AND TPM MANAGEMENT FOR THE HELP DESK

MBAM also provides an Admin website designed to help Tier 1 and Tier 2 help desks/IT Professionals support enterprise BitLocker key recovery.

In this exercise, we will look at how Tier 1 and Tier 2 help desks/IT Professionals can support a user who has lost their PIN and has led to a drive lock-out.

Tasks	Detailed steps
<p>1. Modify the MBAM Recovery page user groups</p>	<p>Perform the following on <b>DC</b>.</p> <p>Roles and permissions to the MBAM Key Recovery page are configured using local groups on the web server. In this first task we will delegate different levels of permissions to two IT professionals: Scott who is Tier 1 and Ed who is Tier 2.</p> <ol style="list-style-type: none"> <li>1. Mouse to the upper right corner to open the <b>Charms</b> bar. Select the <b>Search Charm</b>.</li> <li>2. In the search field type: <b>Users and Computers</b>.</li> <li>3. In the results field, click the <b>Active Directory Users and Computers</b> tile.</li> <li>4. Ensure Users is selected and then in the details pane, double-click <b>MBAMHelpdesk</b>.</li> </ol> <p>This permission tier of the recovery website requires Help Desk personnel to have a User ID and Key ID in order to retrieve recovery information. This group is used to authorize tier1 support who work directly with desktop users in recovery scenarios requiring more input from the end user..</p> <ol style="list-style-type: none"> <li>5. Click <b>Add</b>.</li> <li>6. Type <b>Contoso\Scott</b> and click <b>Check Names</b>.</li> <li>7. Click <b>OK</b> twice.</li> </ol> <p>This permission tier of the recovery website requires the Help Desk Administrator to retrieve recovery information without needing a User ID. This group is used to allow tier 2 support staff direct access to encrypted resources outside of typical user support scenarios.</p> <ol style="list-style-type: none"> <li>8. In the details pane, double-click <b>MBAMAdvancedHelpdesk</b>.</li> <li>9. Click <b>Add</b>.</li> <li>10. Type <b>Contoso\Ed</b> and click <b>Check Names</b>.</li> <li>11. Click <b>OK</b> twice.</li> <li>12. Close Computer Management.</li> </ol>
<p>2. Using the Drive Recovery page in the IT Help Desk role</p>	<p>Perform the following on <b>SVR1</b></p> <ol style="list-style-type: none"> <li>1. Mouse to the upper right corner to open the <b>Charms</b> bar, select the <b>Start</b> charm.</li> <li>2. Click the users name in the top right, select <b>Sign Out</b>.</li> <li>3. Log on as <b>Contoso\Scott</b> with a password of <b>Password1</b>.</li> </ol> <p>In this context we will be logging on in the Help Desk role. The help desk personnel will require both a User ID and a Key ID from the desktop user in order to retrieve recovery information.</p> <ol style="list-style-type: none"> <li>1. Launch the <b>MBAM Help Desk</b> website from the desktop.</li> </ol>

	<p>The BitLocker Administration &amp; Monitoring page appears.</p> <p>2. In the navigation pane, click <b>Drive Recovery</b>.</p> <p>The BitLocker Drive Recovery page allows support staff to access key recovery information without the need to escalate to senior IT Administrators or grant help desks users with access to Active Directory data.</p> <p>3. Enter the following information on the Unlock a Bitlocker Encrypted Drive page:  Domain: <b>CONTOSO</b>  User ID: <b>Administrator</b>  Key ID: <b>cfb9a8c4</b>  Reason for Drive Unlock: <b>Lost PIN</b></p> <p>4. Click <b>Submit</b>.</p> <p>The Drive Recovery Key will display below.</p> <p>5. Close Internet Explorer.</p> <p>6. Logoff of the <b>SVR1</b> machine.</p>
<p>3. Using the Drive Recovery page in the IT Administrator role</p>	<p>1. Log on to the <b>SVR1</b> machine as <b>Contoso\Ed</b> with a password of <b>Password1</b>.</p> <p>Here we are logged in as an IT administrator seeking recovery information outside of the context of user recovery. IT administrators only require a Key ID in order to retrieve recovery information.</p> <p>2. Launch the <b>MBAM Help Desk</b> website from the desktop.</p> <p>The BitLocker Administration &amp; Monitoring page appears.</p> <p>3. In the navigation pane, click <b>Drive Recovery</b>.</p> <p>4. Enter the following information on the Unlock a Bitlocker Encrypted Drive page:  Key ID: <b>cfb9a8c4</b>  Reason for Drive Unlock: <b>Operating System Boot Order changed</b></p> <p>5. Click <b>Submit</b>.</p> <p>6. The Drive Recovery Key will display below.</p> <p>7. Click <b>Save</b>.</p> <p>8. At the Internet Explorer prompt, click the drop down and select <b>Save As</b> and save the text file to the desktop.</p> <p>This will create a recovery key text file that the help desk can send to the user via their email client so it can be read on their phone or another computer.</p> <p>The <b>Save Package</b> option allows for the creation of a <b>Key Package</b>. The <b>Key Package</b> can be used in conjunction with the BitLocker Repair Tool to recover data from a damaged volume. Administrators can use the repair-bde command with the <b>-KeyPackage</b> option.</p> <p>9. Close the download prompt.</p>
<p>4. Using the Manage TPM page</p>	<p>1. Click <b>Manage TPM</b>.</p> <p>The Manage TPM form allows administrators to retrieve the TPM Owner Password File when a TPM has locked users out and no longer accepts user PIN's. Administrators can use this to reset a PIN lockout or perform TPM management tasks.</p>

## LEARN MORE

Thank you for taking the time to learn about Microsoft BitLocker Administration and Monitoring. More information on Microsoft BitLocker Administration and Monitoring (MBAM) can be found online:

Microsoft BitLocker Administration and Monitoring (MBAM) on Microsoft:

<http://www.microsoft.com/windows/enterprise/products/mdop/mbam.aspx>

Windows Client TechCenter > Home > Microsoft Desktop Optimization Pack:

<http://technet.microsoft.com/en-us/windows/bb899442.aspx>

The Official MDOP Blog:

<http://blogs.technet.com/b/mdop>