

ADVANTECH

McAfee® ePolicy Orchestrator® Drive Encryption Quick Start Guide

Release 1.0
2015/9/23

Installation requirements

- Download the latest DriveEncryption v7 product
- Ensure your ePO server version is at least 5.1.
- Ensure your ePO agent version is at least 4.8.
- Note the hostname or IP address of an Active Directory Domain Controller / AD Server

the latest DriveEncryption v7 product

- The downloaded package should contains
 - MDE ePO Extensions
 - Drive Encryption Admin 7.1.3
 - Drive Encryption for PC 7.1.3
 - Drive Encryption Go 7.1.3 (optional)
 - Drive Encryption Help
 - Drive Encryption Out Of Band Management 7.1.1 (for Deep Command)
 - User Directory 1.0.0 (optional)
 - MDE Software Packages
 - Drive Encryption for PC 7.1.3
 - Drive Encryption Go 7.1.3 (optional)
 - Drive Encryption Host 7.1.3

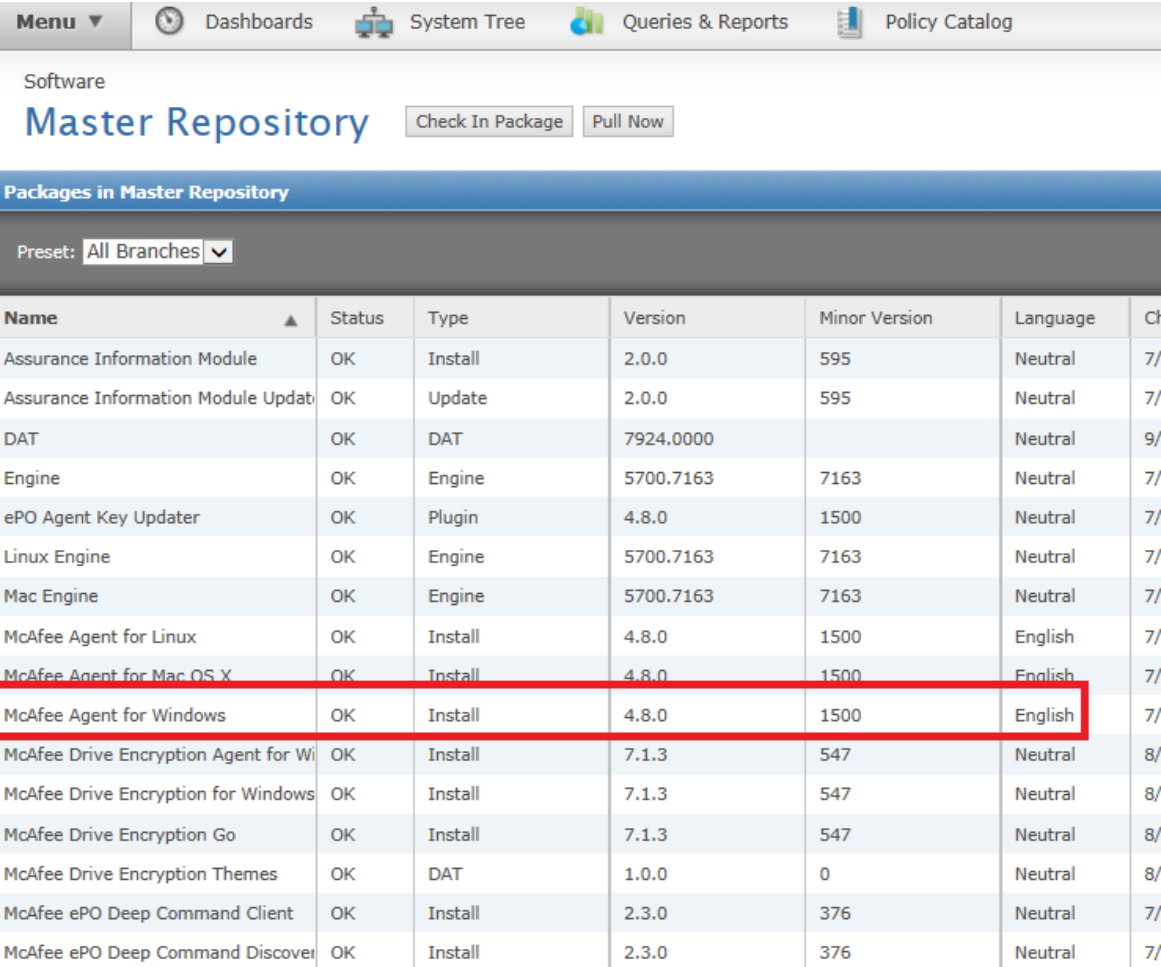
Ensure your ePO server version is at least 5.1

- Click ePO Menu and you can get ePO version

The screenshot displays the ePO interface with a top navigation bar containing 'Menu', 'Dashboards', 'System Tree', 'Queries & Reports', and 'Policy Catalog'. A left sidebar lists 'Recent Pages' (Dashboards, System Tree, Master Repository, Product Deployment, Extensions) and 'Page Description'. The main content area is divided into several sections: Reporting (Dashboards, Queries & Reports, Threat Event Log, McAfee Labs, Solidcore Events, Solidcore Alerts, Content Change Tracking), Systems Section (System Tree, Tag Catalog), Policy (Policy Catalog, Policy Assignments, Policy Assignment Rules, Policy Comparison, Client Task Catalog, Client Task Assignments, Client Task Comparison), Software (Product Deployment, Software Manager, Master Repository, Distributed Repositories, Extensions, Licensing), Automation (Server Task Log, Server Tasks, Automatic Responses, Issues, Solidcore Client Task Log), Data Protection (Encryption Users, Encryption Recovery), User Management (Users, Permission Sets), Configuration (Server Settings, Personal Settings), and Application Control (Inventory, Image Deviation). A red box highlights the version information at the bottom left: 'ePO Build: ePolicy Orchestrator 5.1.1 (Build: 357)'. Below this, server and user details are shown: 'Server: WIN-PRR6C05CMLG', 'Time: 9/18/15 10:58:52 AM PDT', and 'User: admin'.

Ensure your ePO agent version is at least 4.8

- Click Menu=>Master Repository, to check McAfee Agent for windows



Software

Master Repository

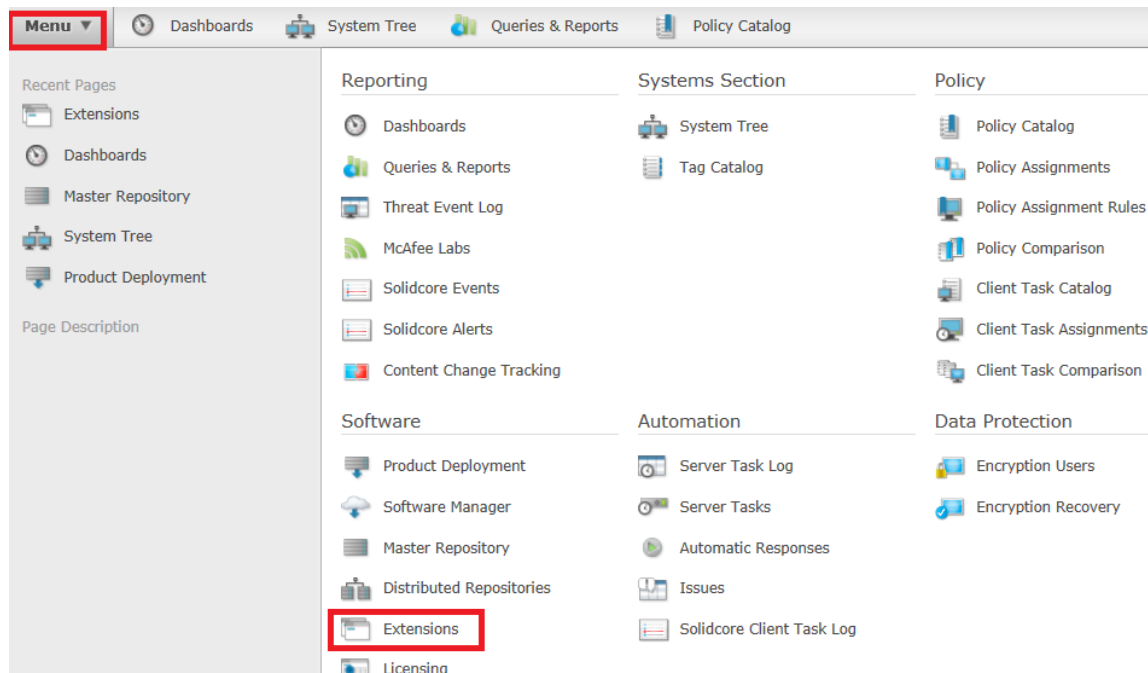
Packages in Master Repository

Preset: ▼

Name ▲	Status	Type	Version	Minor Version	Language	Ch...
Assurance Information Module	OK	Install	2.0.0	595	Neutral	7/
Assurance Information Module Updat	OK	Update	2.0.0	595	Neutral	7/
DAT	OK	DAT	7924.0000		Neutral	9/
Engine	OK	Engine	5700.7163	7163	Neutral	7/
ePO Agent Key Updater	OK	Plugin	4.8.0	1500	Neutral	7/
Linux Engine	OK	Engine	5700.7163	7163	Neutral	7/
Mac Engine	OK	Engine	5700.7163	7163	Neutral	7/
McAfee Agent for Linux	OK	Install	4.8.0	1500	English	7/
McAfee Agent for Mac OS X	OK	Install	4.8.0	1500	English	7/
McAfee Agent for Windows	OK	Install	4.8.0	1500	English	7/
McAfee Drive Encryption Agent for Wi	OK	Install	7.1.3	547	Neutral	8/
McAfee Drive Encryption for Windows	OK	Install	7.1.3	547	Neutral	8/
McAfee Drive Encryption Go	OK	Install	7.1.3	547	Neutral	8/
McAfee Drive Encryption Themes	OK	DAT	1.0.0	0	Neutral	8/
McAfee ePO Deep Command Client	OK	Install	2.3.0	376	Neutral	7/
McAfee ePO Deep Command Discover	OK	Install	2.3.0	376	Neutral	7/

Installation Extensions

- Install the Endpoint Encryption extensions, in this order:
 1. EEADMIN.ZIP (Drive Encryption Admin 7.1.3)
 2. EEPC.ZIP (Drive Encryption for PC 7.1.3)
 3. help_DE_710.100.ZIP (Drive Encryption Help)
- Click Menu=>Software=>Extensions



Installation Extensions

- Click Install Extensions The Install Extension dialog box appears=> Click Browse and select the extension file (3 zip files listed above) then click OK
- The Install Extension page appears with the extension name and version details.

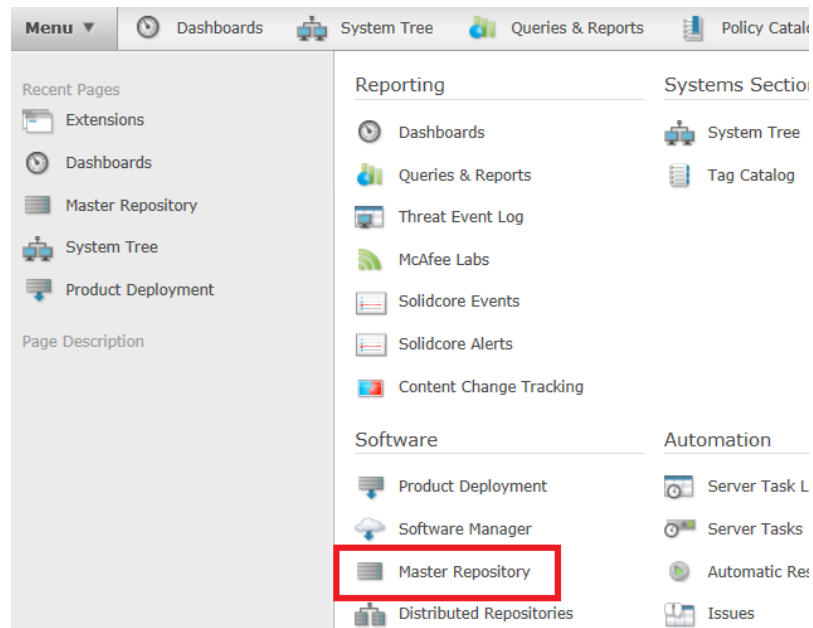
The screenshot displays the 'Install Extension' page in a management console. The page is titled 'Software Extensions' and features a navigation menu on the left with categories like 'McAfee' and 'Third Party'. The main content area lists four installed extensions with their respective details:

Name	Version	Installed by	Status	Requires	Modules
cce_help	3.6.0.010	admin - July 22, 2015 10:11:31 AM PDT	Installed		Core Modules 2.5
deep_command_help	230.016	admin - August 14, 2015 1:10:08 PM PDT	Installed		
de_help	710.100	admin - August 25, 2015 10:20:45 AM PDT	Installed		Core Modules 2.5
epo_help	5.1.0.124	admin - July 17, 2015 5:14:58 PM PDT	Installed		Core Modules 3.0

A red box highlights the 'Install Extension' button at the bottom left of the page.

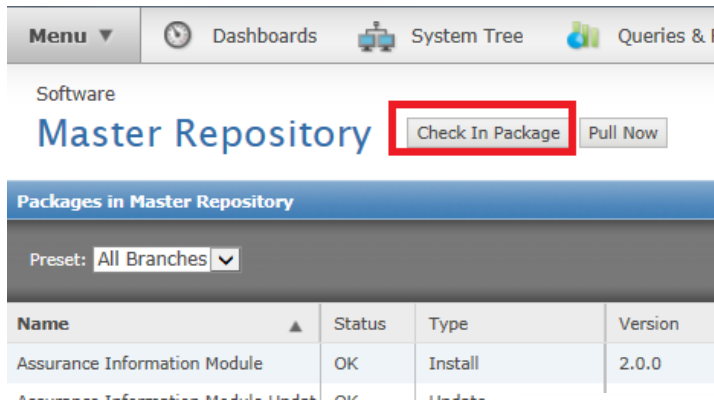
Install Software Package

- Check in the Endpoint Encryption packages, in this order:
 1. MfeEEAgent.zip (Drive Encryption for PC 7.1.3)
 2. MfeEEPC.zip (Drive Encryption Host 7.1.3)
- Click Menu => Software => Master Repository



Install Software Package

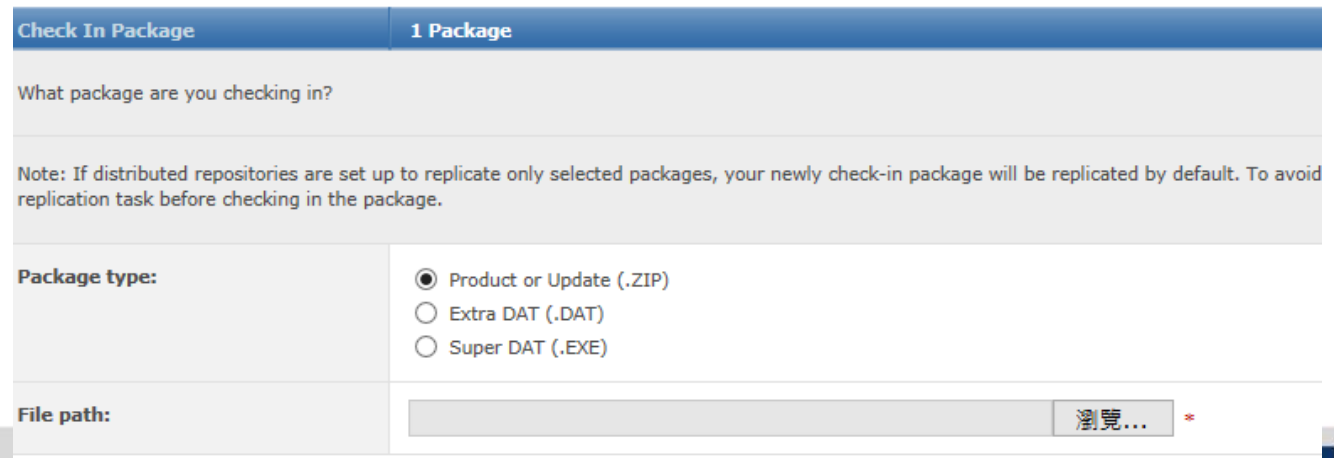
- Click Check In Package. The Check In Package wizard opens.



The screenshot shows the 'Master Repository' page in a software management application. The navigation bar includes 'Menu', 'Dashboards', 'System Tree', and 'Queries & Reports'. The main content area is titled 'Software Master Repository' and features a 'Check In Package' button highlighted with a red box, along with a 'Pull Now' button. Below this is a section for 'Packages in Master Repository' with a 'Preset: All Branches' dropdown. A table lists packages with columns for Name, Status, Type, and Version.

Name	Status	Type	Version
Assurance Information Module	OK	Install	2.0.0
Assurance Information Module Update	OK	Update	

Master Repository



The 'Check In Package' wizard dialog box is shown, titled 'Check In Package' and '1 Package'. It contains the following elements:

- Question: 'What package are you checking in?'
- Note: 'Note: If distributed repositories are set up to replicate only selected packages, your newly check-in package will be replicated by default. To avoid replication task before checking in the package.'
- Package type: Radio buttons for 'Product or Update (.ZIP)' (selected), 'Extra DAT (.DAT)', and 'Super DAT (.EXE)'.
- File path: A text input field with a '瀏覽...' (Browse) button and a red asterisk icon.

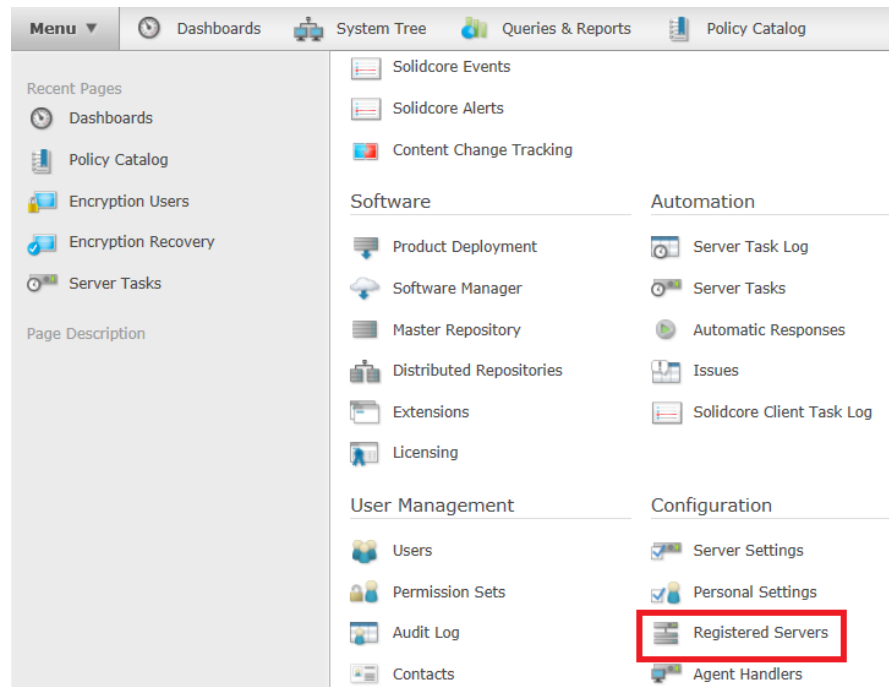
Install Software Package

- Select Product or Update (.ZIP) from the Package type list, then browse to and select the package file (2 zip files listed above).
- Click Next. The Package Options page appears.
- Click Save to begin checking in the package. Wait while the package is checked in.
- The new package appears in the Packages in Master Repository list on the Master Repository page

Mac Engine	OK	Engine	5/00./7163	/7163	Neutral	7/22/15 2:46:29 AM	W
McAfee Agent for Linux	OK	Install	4.8.0	1500	English	7/17/15 5:15:51 PM	W
McAfee Agent for Mac OS X	OK	Install	4.8.0	1500	English	7/17/15 5:16:09 PM	W
McAfee Agent for Windows	OK	Install	4.8.0	1500	English	7/17/15 5:16:27 PM	W
McAfee Drive Encryption Agent for Wi	OK	Install	7.1.3	547	Neutral	8/12/15 4:02:36 PM	M
McAfee Drive Encryption for Windows	OK	Install	7.1.3	547	Neutral	8/12/15 3:50:46 PM	M
McAfee Drive Encryption Go	OK	Install	7.1.3	547	Neutral	8/25/15 10:26:16 AM	M

Registering Windows Active Directory

- Use this option to register a Windows Active Directory. You must have a registered AD to use Policy Assignment Rules, and to enable user permission.
- Click Menu => Configuration => Registered Servers



Registering Windows Active Directory

- Click New Server

The screenshot displays the 'Registered Servers' configuration page. The top navigation bar includes 'Menu', 'Dashboards', 'System Tree', 'Queries & Reports', and 'Policy Catalog'. The main content area is titled 'Registered Servers' and features a left-hand navigation pane with a search filter and a tree view of server categories: 'ePO Servers', 'Ldap Servers', and 'Application Control GTI Cloud S...'. The right-hand pane shows a table with details for the selected server 'WIN-PRR6CO5CMLG (local ePO server)'. The 'New Server' button at the bottom left is highlighted with a red box.

Registered Servers	
Name:	WIN-PRR6CO5CMLG (local ePO server)
Server type:	ePO
Notes:	Registered server for local ePO server

Registering Windows Active Directory

- Select LDAP Server in Server type, specify Server name and click Next

Configuration
Registered Servers

Registered Server Builder	1 Description	2 Details
Server type:	<input type="text" value="LDAP Server"/>	
Name:	<input type="text" value=""/>	*
Notes:	<input type="text" value=""/>	

Back Next Cancel

Registering Windows Active Directory

- Select Active Directory in LDAP server type, type your domain name in Server name, ex: epodomain.com

Configuration

Registered Servers

Registered Server Builder	1 Description	2 Details
LDAP server type:	Active Directory ▼	
Server name:	<input checked="" type="radio"/> Domain name: <input type="text" value="epodomain.com"/> Use DNS-style domain name.	
	<input type="radio"/> Server name: <input type="text"/> Use servername or IP address.	

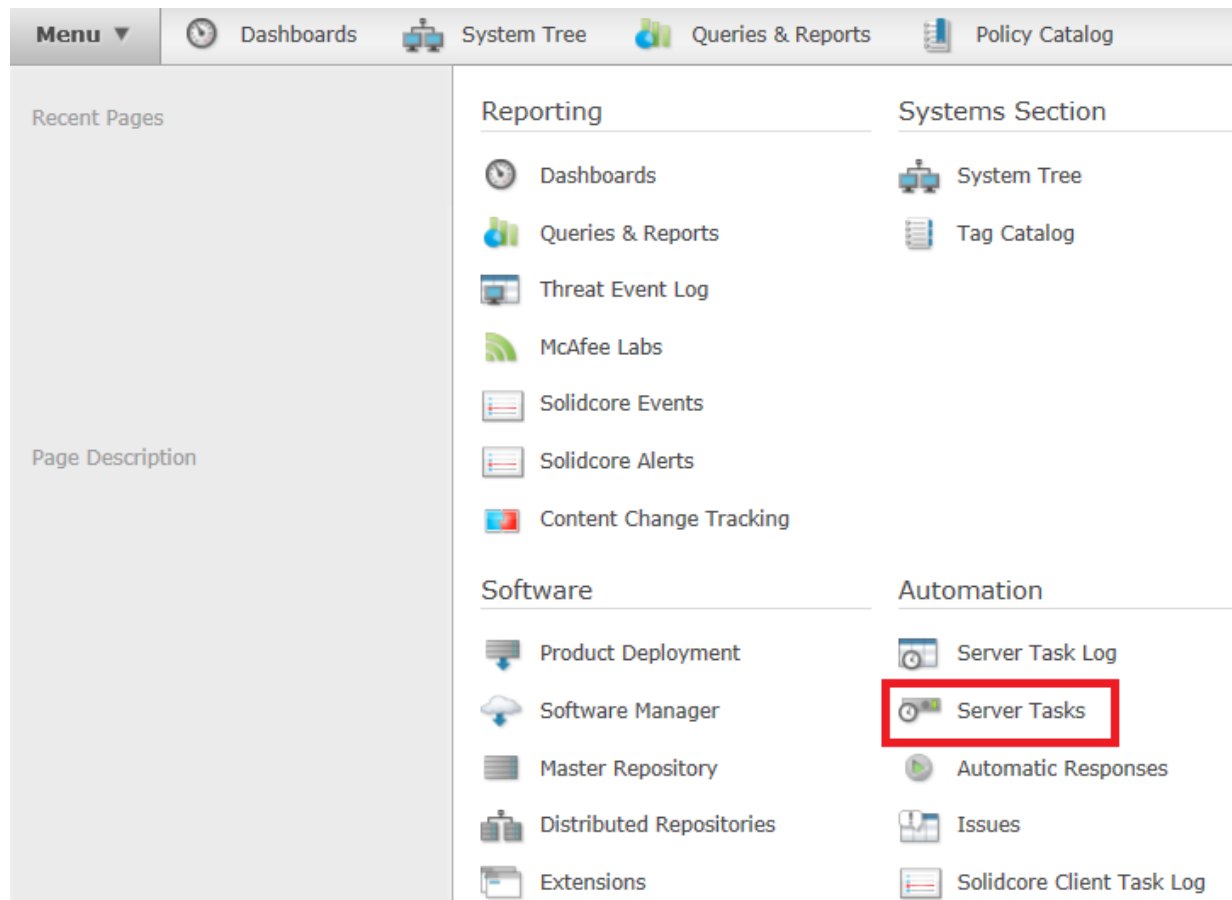
Registering Windows Active Directory

- Type domain user name and password.in User name and password. User name format should be domain\username.
- Click test Connection to check LDAP server connection.
- Click Save to complete.

User name:	<input type="text" value="epodomain/administrator"/>	Use domain\username for Active Directory accounts.
Password:	<input type="password" value="....."/>	
	Confirm password:	<input type="password" value="....."/>
Site name:	<input type="text"/>	<input type="button" value="Browse"/>
<input type="button" value="Test Connection"/>	Successfully connected to the LDAP server.	

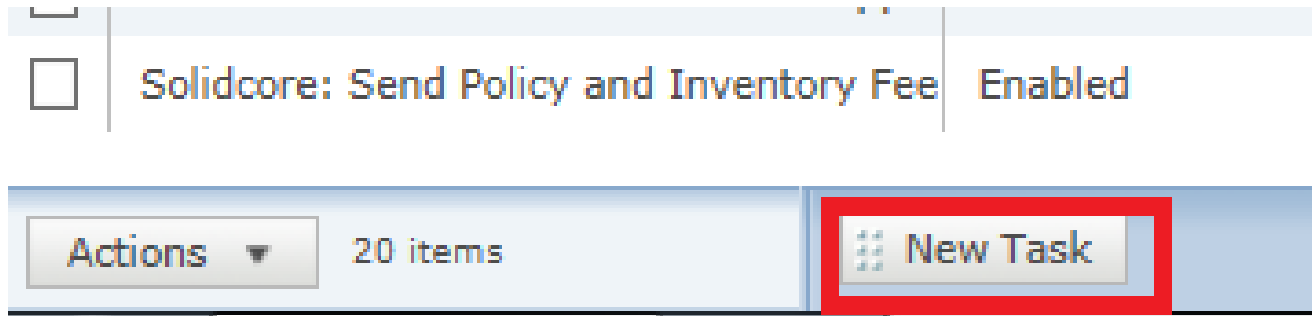
Configuring automation task for LDAP synchronization

- Click Menu => Automation => Server Tasks



Configuring automation task for LDAP synchronization

- Click New task



Configuring automation task for LDAP synchronization

- Naming the task name “Sync LDAP” and click Next

Automation
Server Tasks

Server Task Builder

1 Description 2 Actions 3 Schedule 4 Summary

Name:	<input type="text" value="Sync LDAP"/>
Notes:	<input type="text"/>
Schedule status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

Back **Next** Cancel

Configuring automation task for LDAP synchronization

- In Action, please select LdapSync:sync across users from LDAP
- Select LDAP server is to select the server you create in last chapter. After that, click Next

Automation
Server Tasks

Server Task Builder

1 Description > 2 Actions > 3 Schedule > 4 Summary

What actions do you want the task to take?

1. Actions: LdapSync: Sync across users from LDAP

Select LDAP Server: All Servers

Back Next

Configuring automation task for LDAP synchronization

- Just follow the default and click Next

Automation
Server Tasks

Server Task Builder

1 Description > 2 Actions > 3 Schedule > 4 Summary

Schedule type: Daily

Start date: 09 / 21 / 2015

End date:
 09 / 22 / 2015
 No end date

Schedule: at 1 : 00 AM

Back Next

Configuring automation task for LDAP synchronization

- Click Save to save this task

Automation
Server Tasks

Server Task Builder 1 Description 2 Actions 3 Schedule 4 Summary

Name:	Sync LDAP
Notes:	No notes available
Task owner:	admin
Schedule status:	Enabled
Schedule:	Start date: 9/21/15 End date: No end date Time frame: Daily at 1:00 AM Next run time: 9/22/15 1:00 AM 9/23/15 1:00 AM 9/24/15 1:00 AM
Actions:	1. LdapSync: Sync across users from LDAP [test] will be synced to the desired schedule.

Back Save

Configure Client Tasks to Deploy the Endpoint Encryption Agent

- Please follow ePO SOP to add a client to manage.
- In system tree, select the client system and click Action =>Agent=>Run Client task Now

The screenshot displays the ePO console interface. A table lists managed systems, with 'CCC-PC' selected. A context menu is open over the 'Agent' category, and the 'Run Client Task Now' option is highlighted with a red box. The 'Actions' menu at the bottom is also highlighted with a red box, showing '1 of 1 selected'.

<input type="checkbox"/>	System Name	Managed State	Tags
<input checked="" type="checkbox"/>	CCC-PC	Managed	AMT, Workstation

- Choose Columns
- Drive Encryption
- Drive Encryption Go
- Export Table
- Tag
- AMT Actions
- Application Control
- Agent**
- Directory Management

- Deploy Agents
- Modify Policies on a Single System
- Modify Tasks on a Single System
- Run Client Task Now**
- Set Description
- Set Policy & Inheritance
- Show Agent Log
- Show Client Events
- Show Threat Events
- Transfer Systems
- Update Now
- Wake Up Agents

Actions ▼ 1 of 1 selected

Wake Up Agents Ping

Configure Client Tasks to Deploy the Endpoint Encryption Agent

- In product, please select McAfee Agent=>Product Deployment=>Create New Task

Systems Section
System Tree

Run Client Task Now

Select a task object from the list of Tasks and set additional options for the task under the "Options" tab below. Note that "Run Now" tasks will only work on Microsoft Windows operating systems.

Product	Task Type	Task Name
Filter list...	Filter list...	Filter list...
ePO Deep Command 2.3.0	McAfee Agent Statistics	Deploy ePO Deep Command Client
McAfee Agent	McAfee Agent Wakeup	Deploy ePO Deep Command Discovery and Reporting Plugin
Solidcore 6.1.3	Mirror Repositories (Windows only)	DeploySolidcore
	Product Deployment	Metering Deployment Task
	Product Update	Create New Task

Affected Systems | Options | Ignored Systems

Configure Client Tasks to Deploy the Endpoint Encryption Agent

- Select McAfee Drive Encryption Agent for windows and click “+” and select McAfee Drive Encryption for Windows. =>Run Task Now

Systems Section
System Tree

Run Client Task Now

Target platforms:

- AIX
- Email and Web Security Appliances
- HP-UX
- Linux
- Mac
- McAfee Linux OS
- Solaris
- Wind River Linux
- Windows

Products and components:

McAfee Drive Encryption Agent for Windows 7.1.3.547 Action: Install Language: Language Neutral Branch: Current - +

Command line:

McAfee Drive Encryption for Windows 7.1.3.547 Action: Install Language: Language Neutral Branch: Current - +

Command line:

"Postpone Deployment" dialog box (Windows systems only):

- Allow end users to postpone this deployment
- Maximum number of postpones allowed:
- Option to postpone expires after (seconds):
- Display this text:

Run Task Now

Configure Client Tasks to Deploy the Endpoint Encryption Agent

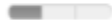
- To check the status and click Close

Systems Section

System Tree

Running Client Task Status

Running Task: McAfee Agent > Product Deployment > McAfee Agent > Product Deployment
Initiated: 9/21/15 3:31:00 PM by admin

System	Status
▶ My Organization > Test > CCC-PC	

Configure Client Tasks to Deploy the Endpoint Encryption Agent

- After completed install, client will be reboot itself.
- After client reboot, click agent => About, you can see drive encryption agent and drive encryption



Configure Client Tasks to Deploy the Endpoint Encryption Agent

- Agent => Quick Settings => Show Drive Encryption Status, You can see System State is inactive



Add Group Users

- Menu => Data Protection => Endpoint Encryption Users

The screenshot displays the Advantech management console interface. At the top, there is a navigation bar with a 'Menu' dropdown and several main sections: 'Dashboards', 'System Tree', 'Queries & Reports', and 'Policy Catalog'. Below this, the interface is divided into several columns. On the left, there is a sidebar with 'Recent Pages' (including 'Encryption Users', 'System Tree', 'Dashboards', 'Server Tasks', and 'Registered Servers') and a 'Page Description' for 'Encryption Users' which reads 'Assign users to machine for disk encryption'. The main content area is organized into four sections: 'Reporting' (containing Dashboards, Queries & Reports, Threat Event Log, McAfee Labs, Solidcore Events, Solidcore Alerts, and Content Change Tracking), 'Systems Section' (containing System Tree and Tag Catalog), 'Automation' (containing Server Task Log, Server Tasks, and Automatic Responses), and 'Data Protection' (containing Policy Catalog, Policy Assignments, Policy Assignment Rules, Policy Comparison, Client Task Catalog, Client Task Assignments, Client Task Comparison, and 'Encryption Users'). The 'Encryption Users' item in the 'Data Protection' section is highlighted with a red border and a yellow background. A tooltip is visible over the 'Encryption Users' icon, showing the text 'Encryption Users'.

Add Group Users

- Actions=>Drive Encryption=>Add User

Data Protection
Encryption Users

System Tree

- My Organization
 - AMT devices
 - DeploySolidcore
 - Enable_Solidcore
 - none
 - Pull Inventory
 - Test
 - unconfigure
 - Lost&Found

My Organization > Test

Systems Group Users

Systems : System Users

Preset: This Group Only Custom: None Quick find:

<input type="checkbox"/>	System Name	Tags
<input checked="" type="checkbox"/>	CCC-PC	AMT, Workstation

Choose Columns

Drive Encryption

Export Table

Add User(s)

View Users

Tasks




Actions 1 of 1 selected

Add Group Users

- Click open folder icon

Data Protection
Encryption Users

Add Drive Encryption Users

Users:	<input type="text"/>  *
From the groups:	<input type="text"/>  * <input type="checkbox"/> Recursive
From the organizational units:	<input type="text"/>  * <input type="checkbox"/> Recursive

Add Group Users

- Select LDAP server in Look in, and extract the existed domain group

The screenshot shows a web interface for selecting users. At the top, there is a 'Select Users' header. Below it, a 'Look in:' dropdown menu is set to 'test'. To the left, a 'Browse Groups' sidebar shows a tree view with 'epodomain' selected. The main area is titled 'Users (limited to 2,000 records)' and contains a 'Preset: Container only' dropdown, a 'Quick find:' search box, and 'Apply' and 'Clear' buttons. Below these controls is a table with three columns: 'Name', 'Attribute', and 'Distinguished Name'. The table is currently empty, and a 'No results found' message is displayed at the bottom.

Name	Attribute	Distinguished Name
No results found		

Add Group Users

- Choose Users and check Administrator, and click OK

Select Users

Look in: test

Browse Groups

- epodomain
- Builtin
- Computers
- Domain Controllers
- ForeignSecurityPrincipals
- Managed Service Accounts
- Program Data
- System
- Users

Users (limited to 2,000 records)

Hide Filter

Preset: Container only Quick find: Apply Clear Show selected rows

	Name	Attribute	Distinguished Name
<input checked="" type="checkbox"/>	Administrator	Administrator	CN=Administrator,CN=Users,DC=epodomain,DC=com
<input type="checkbox"/>	Guest	Guest	CN=Guest,CN=Users,DC=epodomain,DC=com
<input type="checkbox"/>	krbtgt	krbtgt	CN=krbtgt,CN=Users,DC=epodomain,DC=com
<input type="checkbox"/>	lin roger	rogerlin	CN=lin roger,CN=Users,DC=epodomain,DC=com

OK Cancel




Add Group Users

- Click OK to complete add group user

Data Protection

Encryption Users

Add Drive Encryption Users

Users:	<input type="text" value="CN=Administrator,CN=Users,DC=epodomain,DC="/> 
From the groups:	<input type="text"/>  <input type="checkbox"/> Recursive
From the organizational units:	<input type="text"/>  <input type="checkbox"/> Recursive

Configure EEPC Product Settings Policy

- Click system tree, click group in left pane, and click Assigned Policies

The screenshot shows the EEPC System Tree interface. The top navigation bar includes 'Menu', 'Dashboards', 'System Tree' (highlighted with a red box), 'Queries & Reports', and 'Policy Catalog'. Below the navigation bar, the 'System Tree' section is visible, with 'New Systems' and 'New Subgroups' buttons. The 'System Tree' pane on the left lists various system groups, with 'unconfigure' highlighted in yellow and a red box. The main pane shows the 'Assigned Policies' tab, with 'Preset: This Group Only' and 'Custom: None' dropdowns. A table below displays the assigned policies for the selected system.

	<input type="checkbox"/>	System Name ▲	Managed State	Tags
	<input type="checkbox"/>	CCC-PC	Managed	Workstation

Configure EEPC Product Settings Policy

- Select product: Drive Encryption 7.1.3 and to check it show Product Settings and User Based Policies

The screenshot shows the EEPC System Tree interface. The top navigation bar includes Menu, Dashboards, System Tree, Queries & Reports, and Policy Catalog. The main area is titled 'Systems Section' and 'System Tree', with buttons for 'New Systems' and 'New Subgroups'. The 'System Tree' sidebar on the left lists various system categories, with 'unconfigure' highlighted in yellow. The main content area is divided into tabs: 'Systems', 'Assigned Policies', 'Assigned Client Tasks', 'Group Details', and 'Agent Deployment'. The 'Assigned Policies' tab is active, showing a configuration for 'Drive Encryption 7.1.3' with an enforcement status of 'Enforcing'. A table below lists the assigned policies, with 'Product Settings' and 'User Based Policies' highlighted in red.

Category	Policy	Server	Inherit from
Product Settings	My Default	Local (WIN-PRR6CO5CMLG)	My Organization
User Based Policies	My Default	Local (WIN-PRR6CO5CMLG)	My Organization
Add Local Domain User Settin	My Default	Local (WIN-PRR6CO5CMLG)	My Organization

Configure EEPC Product Settings Policy

- Click My Default near Product Settings

Systems Section

System Tree

New Systems New Subgroups

System Tree

Systems Assigned Policies Assigned Client Tasks Group Details Agent Deployment

Product: Drive Encryption 7.1.3 Enforcement status: Enforcing

Category	Policy	Server	Inherit from
Product Settings	My Default	Local (WIN-PRR6CO5CMLG)	My Organization
User Based Policies	My Default	Local (WIN-PRR6CO5CMLG)	My Organization
Add Local Domain User Settings	My Default	Local (WIN-PRR6CO5CMLG)	My Organization

My Organization

- AMT devices
- DeploySolidcore
- Enable_Solidcore
- none
- Pull Inventory
- Test
- unconfigure
- Lost&Found
 - ADVANTECH
 - WORKGROUP

Configure EEPC Product Settings Policy

- In General tab

Systems Section

System Tree

Drive Encryption 7.1.3 > Product Settings > My Default

General Encryption Log On Recovery Boot Options Theme Out-of-Band Encryption Providers Companion Devices

Enable policy: Only activate if health check (Drive Encryption : Go) passes

Logging level: Error, Warnings and Informational

Harden against cold boot attacks when:

- The system is locked.
- The user is logged off.
- The system is in standby.

This feature is only available on systems that support it.

Expire users who do not login: Expiry after 1 hour(s) (1-8640)

Allow users to create endpoint info file:

Configure EEPC Product Settings Policy


- In Encryption Tab


Systems Section
System Tree

Drive Encryption 7.1.3 > Product Settings > My Default

General **Encryption** Log On Recovery Boot Options Theme Out-of-Band Encryption Providers Companion Devices

Encrypt:

To change the priority, grab the handle () and drag the row (highest priority is at the top)

Encryption Provider	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Actions
	None	All disks	Boot disk only	All disks except boot disk	Selected partitions	
PC Opal 	✘	✔	✔	✘	✘	
PC Software	✔	✔	✔	✔	✔	Move To Top

Configure EEPC Product Settings Policy

- In LogOn Tab

Systems Section
System Tree

Drive Encryption 7.1.3 > Product Settings > My Default

General Encryption **Log On** Recovery Boot Options Theme Out-of-Band Encryption Providers Companion Devices

Drive Encryption

Enable automatic booting:	<input type="checkbox"/> <input type="checkbox"/> Until expiration date 09 / 22 / 2015 1 : 00 AM <input type="checkbox"/> Use UTC <input type="checkbox"/> Disable and restart system after 3 (1-10) failed logons or unlocks (Windows only, Vista onwards)
Allow temporary automatic booting:	<input checked="" type="checkbox"/>
Use of TPM for automatic booting:	<input checked="" type="radio"/> Never <input type="radio"/> If available <input type="radio"/> Required (Note: if TPM is not available on the system, automatic booting will not be enabled)
Pre-boot power management:	<input type="checkbox"/> Automatically shutdown pre-boot after a period of inactivity: 1 (1-60 minutes)
Log on message:	<input type="text"/> (0-3000 characters. This includes non printable characters.)

Configure EEPC Product Settings Policy

- In LogOn Tab

Do not display previous user name at log on:	<input checked="" type="checkbox"/>
Enable on screen keyboard:	<input checked="" type="checkbox"/> <input type="checkbox"/> Always display on screen keyboard
Add local domain users (and tag with 'EE:ALDU'):	<input checked="" type="radio"/> Disabled <input type="radio"/> Add all previous and current local domain users of the system <input type="radio"/> Only add currently logged on local domain user(s); activation is dependent on a successful user assignment
Enable accessibility:	<input type="checkbox"/>
Disable pre-boot authentication when not synchronized:	<input type="checkbox"/> (Requires recovery to be enabled) After <input type="text" value="1"/> days (1-365)
Read username from smartcard:	<input type="checkbox"/> <input type="text" value="Subject"/> is the certificate field which will contain the username <input type="checkbox"/> Match certificate username field up to @ sign

Configure EEPC Product Settings Policy

- In Recovery Tab

Systems Section

System Tree

Drive Encryption 7.1.3 > Product Settings > My Default

General Encryption Log On **Recovery** Boot Options Theme Out-of-Band Encryption Providers Companion Devices

Administrator recovery

Enabled:

Key size: Low

Message: (0-3000 characters. This includes non printable characters.)

Self-recovery

Allow users to re-enroll self-recovery information at PBA:

Configure EEPC Product Settings Policy

- In Boot Options Tab

Systems Section

System Tree

Drive Encryption 7.1.3 > Product Settings > My Default

General Encryption Log On Recovery **Boot Options** Theme Out-of-Band Encryption Providers Companion Devices

Enable Boot Manager:	<input type="checkbox"/> Partition 1 <input type="text" value="1"/> Partition 2 <input type="text" value="2"/> Partition 3 <input type="text" value="3"/> Partition 4 <input type="text" value="4"/> <input checked="" type="checkbox"/> Time out Time out <input type="text" value="30"/> in seconds (1 - 300)
Always enable pre-boot USB support:	<input type="checkbox"/>
Enable pre-boot PCMCIA support:	<input type="checkbox"/>
Graphics mode:	<input type="text" value="Automatic"/> ▼

Configure EEPC Product Settings Policy

- Click Save

Systems Section

System Tree

Drive Encryption 7.1.3 > Product Settings > My Default

General Encryption Log On Recovery **Boot Options** Theme Out-of-Band Encryption Providers Companion Devices

Enable Boot Manager:	<input type="checkbox"/> Partition 1 <input type="text" value="1"/> Partition 2 <input type="text" value="2"/> Partition 3 <input type="text" value="3"/> Partition 4 <input type="text" value="4"/> <input checked="" type="checkbox"/> Time out Time out <input type="text" value="30"/> in seconds (1 - 300)
Always enable pre-boot USB support:	<input type="checkbox"/>
Enable pre-boot PCMCIA support:	<input type="checkbox"/>
Graphics mode:	<input type="text" value="Automatic"/> ▼

Duplicate Save C

Configure EEPC User Based Policy (UBP) Settings

- Click My Default near user based Policies

Systems Section

System Tree

[New Systems](#) [New Subgroups](#)

System Tree

Systems **Assigned Policies** Assigned Client Tasks Group Details Agent Deploy

Product: Drive Encryption 7.1.3 Enforcement status: Enforcin

Category	Policy	Server	Inherit fro
Product Settings	My Default	Local (WIN-PRR6C05CMLG)	My Organ
User Based Policies	My Default	Local (WIN-PRR6C05CMLG)	My Organ
Add Local Domain User Settin	My Default	Local (WIN-PRR6C05CMLG)	My Organ

System Tree

- My Organization
 - AMT devices
 - DeploySolidcore
 - Enable_Solidcore
 - none
 - Pull Inventory
 - Test
 - unconfigure
 - Lost&Found
 - ADVANTECH

Configure EEPC User Based Policy (UBP) Settings

- In Authentication Tab

Systems Section

System Tree

Drive Encryption 7.1.3 > User Based Policies > My Default

Authentication Password Password Content Rules Self-recovery Companion Devices

Token type: Password only

Certificate rule:

- Provide LDAP user certificate
- Enforce certificate validity period on client
- Use latest certificate

Add certificate rule

Logon Hours: Apply restrictions

	Midnight (AM)											Noon (PM)												
Every day	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11
Sunday																								
Monday																								
Tuesday																								
Wednesday																								
Thursday																								
Friday																								
Saturday																								

allow
 block

Configure EEPC User Based Policy (UBP) Settings

- In Password Tab

Systems Section
System Tree

Drive Encryption 7.1.3 > User Based Policies > My Default

Authentication **Password** Password Content Rules Self-recovery Companion Devices

Default password:	<input type="checkbox"/> Change default password Password <input type="text"/> Confirm <input type="text"/> <input type="checkbox"/> Do not prompt for default password
Password change:	<input checked="" type="checkbox"/> Enable password history <input type="text" value="10"/> changes (1-100) <input type="checkbox"/> Prevent change <input type="checkbox"/> Require change after <input type="text" value="30"/> days (1-366) Warn user <input type="text" value="0"/> days before password expires (0-30)
Incorrect passwords:	<input checked="" type="checkbox"/> Timeout password entry after <input type="text" value="3"/> invalid attempts (3-20) Maximum disable time <input type="text" value="64"/> minutes (1-64) <input checked="" type="checkbox"/> Invalidate password after <input type="text" value="10"/> invalid attempts (3-100)
Allow showing of password:	<input type="checkbox"/>

Configure EEPC User Based Policy (UBP) Settings

- In Self Recovery Tab

Systems Section
System Tree

Drive Encryption 7.1.3 > User Based Policies > My Default

Authentication Password Password Content Rules **Self-recovery** Companion Devices

Enable self-recovery:

Invalidate self-recovery after no. of invalid attempts:
No. of attempt : (1-100)

Questions to be answered: (1-10)

Logons before forcing user to set answers: (0-20)

Questions:

English (US)	Question	<input type="text" value="What is your favorite color?"/>	-
Chinese (Traditional)	Min answer length	<input type="text" value="3"/> (1-200)	
Chinese (Simplified)	Question	<input type="text" value="What is your pet's name?"/>	-
Dutch	Min answer length	<input type="text" value="2"/> (1-200)	
French	Question	<input type="text" value="Who is your favorite musician?"/>	-
German	Min answer length	<input type="text" value="2"/> (1-200)	
Greek	Question	<input type="text" value="What is a memorable date?"/>	-
Italian	Min answer length	<input type="text" value="8"/> (1-200)	
Japanese	Question	<input type="text" value="What is your date of birth?"/>	-
Korean			
Brazilian Portuguese			
Portuguese			
Spanish			
Danish			
Estonian			
Finnish			
Norwegian			
Polish			

Configure EEPC User Based Policy (UBP) Settings

- In Companion Devices Tab

Systems Section

System Tree

Drive Encryption 7.1.3 > User Based Policies > My Default

Authentication	Password	Password Content Rules	Self-recovery	Companion Devices
----------------	----------	------------------------	---------------	--------------------------

Recovery: Enabled

Password Definition:

- PIN, exactly 6 digits
- PIN, exactly 8 digits
- Password, minimum 6 with 1 numeric, 1 alphabetic
- Password, minimum 6 with 1 numeric, 1 uppercase and 1 lowercase
- Password, minimum 8 with 1 numeric, 1 uppercase, 1 lowercase and 1 symbol

Configure EEPC User Based Policy (UBP) Settings

- Click Save

Systems Section
System Tree

Drive Encryption 7.1.3 > User Based Policies > My Default

Authentication Password Password Content Rules Self-recovery **Companion Devices**

Recovery: Enabled

Password Definition:

- PIN, exactly 6 digits
- PIN, exactly 8 digits
- Password, minimum 6 with 1 numeric, 1 alphabetic
- Password, minimum 6 with 1 numeric, 1 uppercase and 1 lowercase
- Password, minimum 8 with 1 numeric, 1 uppercase, 1 lowercase and 1 symbol

Duplicate Save Can

Assign policies

- Click System

Systems Section

System Tree

New Systems New Subgroups

System Tree

Systems Assigned Policies Assigned Client Tasks Group Details Ag

Product: Drive Encryption 7.1.3 Enforcement statu

Category	Policy	Server
Product Settings	My Default	Local (WIN-PRR6CO5CMLG)
User Based Policies	My Default	Local (WIN-PRR6CO5CMLG)
Add Local Domain User Setting	My Default	Local (WIN-PRR6CO5CMLG)

▼ My Organization

- AMT devices
- DeploySolidcore
- Enable_Solidcore
- none
- Pull Inventory
- Test
- unconfigure

▼ Lost&Found

Assign policies

- Check system and click Wake Up Agents

The screenshot shows a management interface with a table of systems. At the top, there are dropdown menus for 'Preset: This Group Only' and 'Custom: None'. The table has columns for 'System Name', 'Managed State', and 'Tags'. One system, 'CCC-PC', is selected, indicated by a checked checkbox and a yellow background. Below the table, an 'Actions' bar shows '1 of 1 selected' and a 'Wake Up Agents' button highlighted with a red box.

<input type="checkbox"/>	System Name ▲	Managed State	Tags
<input checked="" type="checkbox"/>	CCC-PC	Managed	Workstation

Actions ▼ 1 of 1 selected **Wake Up Agents** Ping

Assign policies

- Check Force Complete policy and task update and click OK

Systems Section

System Tree

Wake Up McAfee Agent

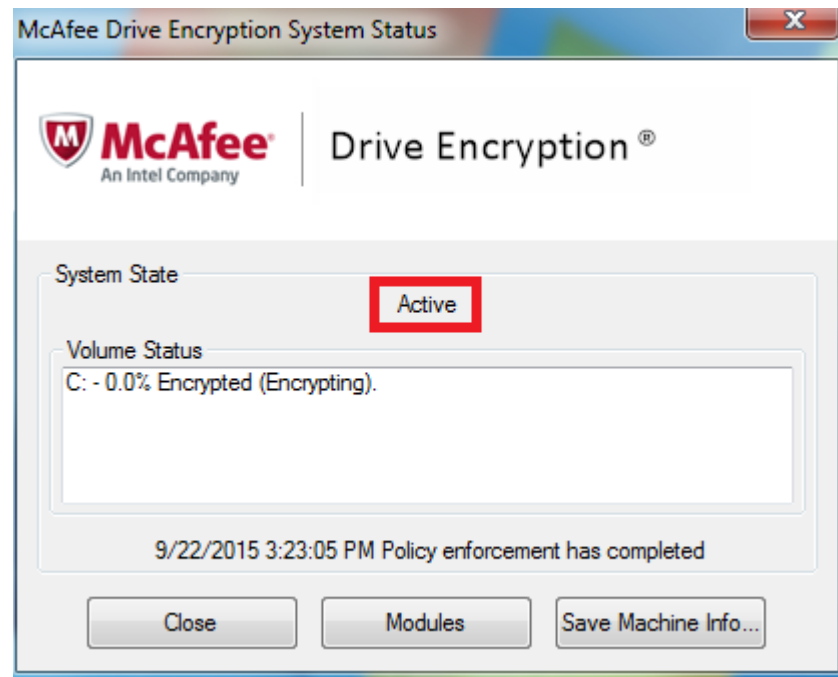
Click "OK" to send the wake-up call to the target systems. To see the status of the wake-up call, go to the Server Task Log.

Target systems:	CCC-PC
Wake-up call type:	<input checked="" type="radio"/> Agent Wake-Up Call <input type="radio"/> SuperAgent Wake-Up Call
Randomization:	<input type="text" value="0"/> minutes
Options:	<input checked="" type="checkbox"/> Retrieve all properties even if they haven't changed since the last time they were collected. If unchecked only retrieve changed properties.
Force policy update:	<input checked="" type="checkbox"/> Force complete policy and task update
Number of attempts:	<input type="text" value="1"/> (Enter 0 for continuous attempts.)
Retry interval:	<input type="text" value="30"/> <input type="text" value="second(s)"/>
Abort after:	<input type="text" value="5"/> <input type="text" value="minute(s)"/>
Wake up Agent using:	<input checked="" type="radio"/> All Agent Handlers <input type="radio"/> Last Connected Agent Handler <input type="radio"/> Selected Agent Handler: <input type="text"/>

OK

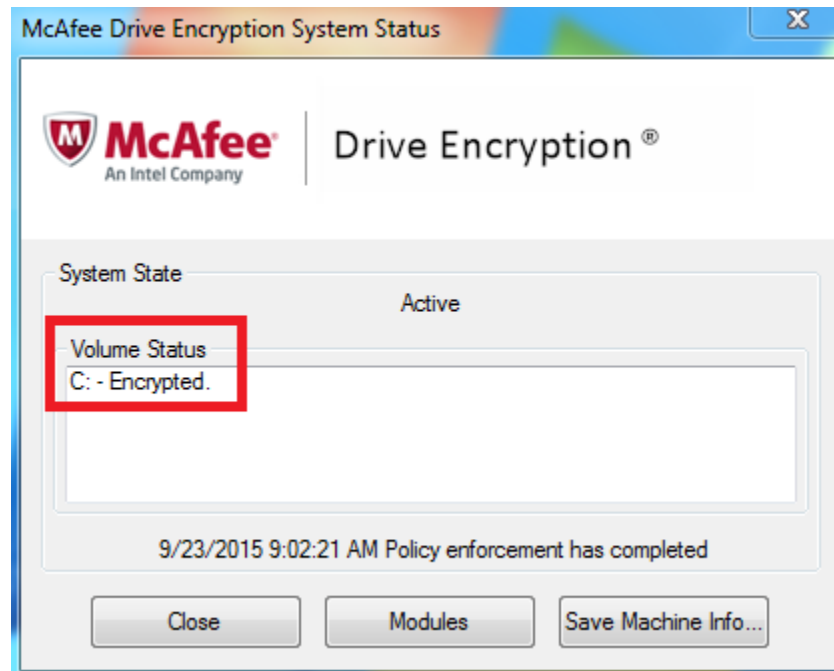
Assign policies

- You can see client Agent => Quick Settings => Show Drive Encryption Status in several minutes and state is Active



Assign policies

- It will take several hours for the first time encryption
- You can see encryption completed



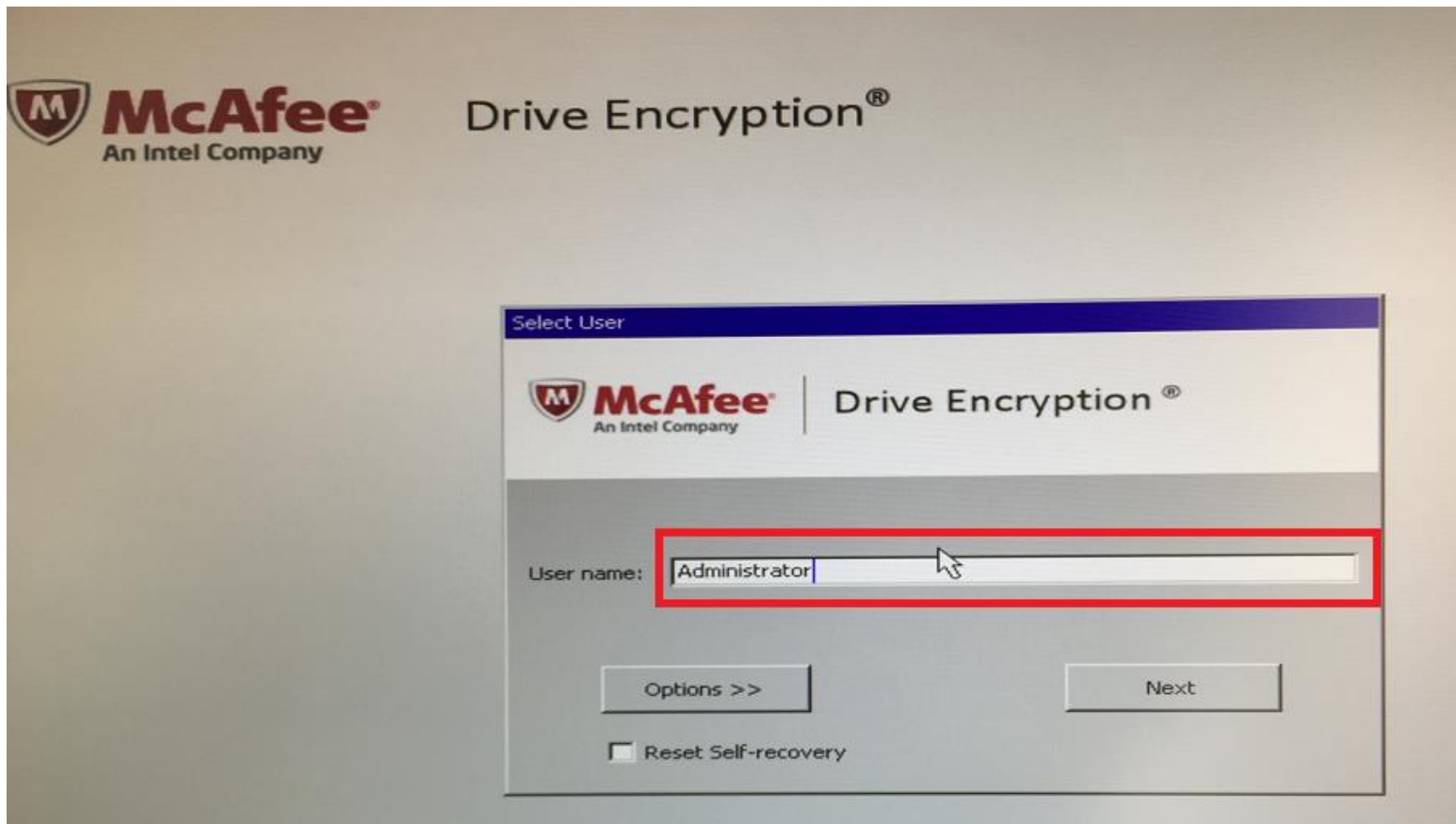
Drive Encryption Login

- After client reboot, you can see Drive Encryption Login



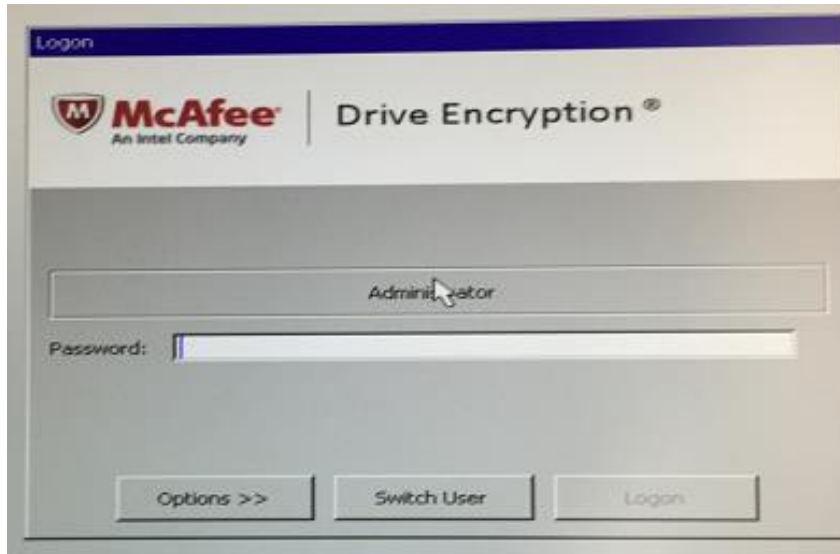
Drive Encryption Login

- Please type Administrator (or you set user in Add Group User section)



Drive Encryption Login

- Default Password: “12345” , after typing the password, system asks you to modify your password.



Drive Encryption Login

- Please answer some question. You need to type these answer if you lost your password.



Self-Recovery Enrollment

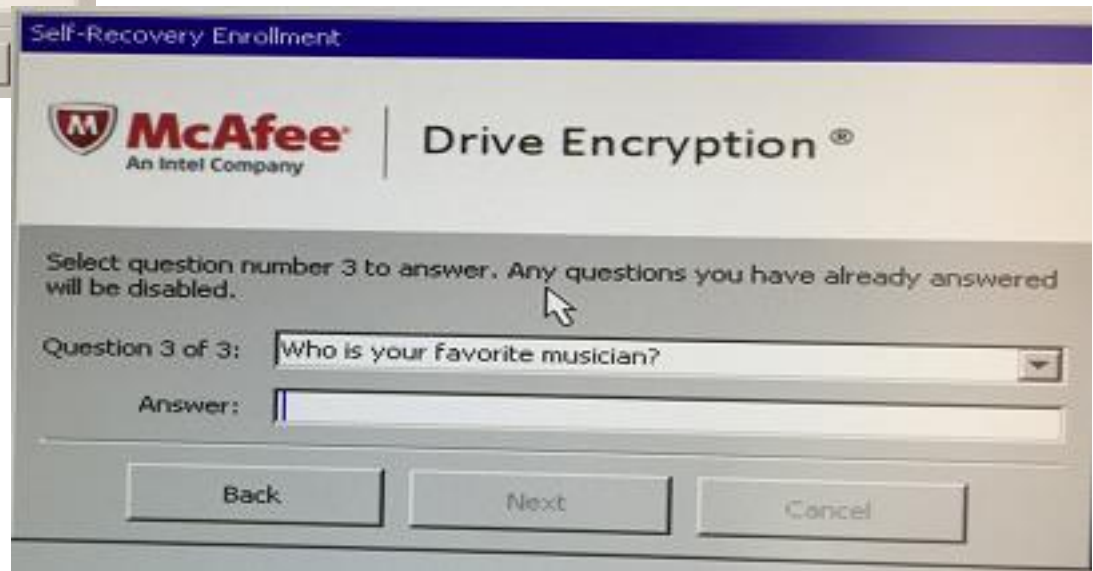
McAfee
An Intel Company | Drive Encryption®

Select question number 1 to answer. Any questions you have already answered will be disabled.

Question 1 of 3: What is your Favorite color?

Answer:

Back Next Cancel



Self-Recovery Enrollment

McAfee
An Intel Company | Drive Encryption®

Select question number 3 to answer. Any questions you have already answered will be disabled.

Question 3 of 3: Who is your favorite musician?

Answer:

Back Next Cancel