SafeNet Authentication Client

Integration Guide

Using SAC CBA with McAfee Drive Encryption

SafeNet

THE
DATA
PROTECTION
COMPANY

Document Information

Document Part Number	007-012690-001, Rev. A
Release Date	October 2014

Trademarks

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording, or otherwise, without the prior written permission of SafeNet, Inc.

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Contents

Introduction

Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as McAfee® Drive Encryption.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Overview

McAfee Drive Encryption provides superior encryption across a variety of endpoints, such as desktops and laptops. The McAfee Drive Encryption solution uses strong access control with pre-boot authentication (PBA) and a NIST-approved algorithm to encrypt data on endpoints. Encryption and decryption are completely transparent to the end user and are performed without hindering system performance.

An effective strong authentication solution must be able to address data breaches. It is important for companies to protect their information assets and comply with privacy regulations. Data encryption is a common technique used by enterprises today, but to be most effective, it must be accompanied by strong two factor user authentication to desktop, mobile, and laptop computer applications. Working together, encryption and authentication reduce risk and stop unauthorized access to sensitive data.

SafeNet Smart Card Certificate-Based Tokens and secure USB Certificate-Based Tokens are now interoperable with McAfee Drive Encryption, the McAfee solution for encryption and strong access control that prevents unauthorized access to sensitive data and stops information loss and exposure. The integrated solution delivers greater security, reduces operational costs, and improves compliance by adding smart cards based strong user authentication to McAfee Drive Encryption.

SafeNet's X.509 certificate-based USB tokens and smartcards have been integrated with McAfee Drive Encryption, providing two-factor authentication at both pre-boot and at Microsoft Windows levels.

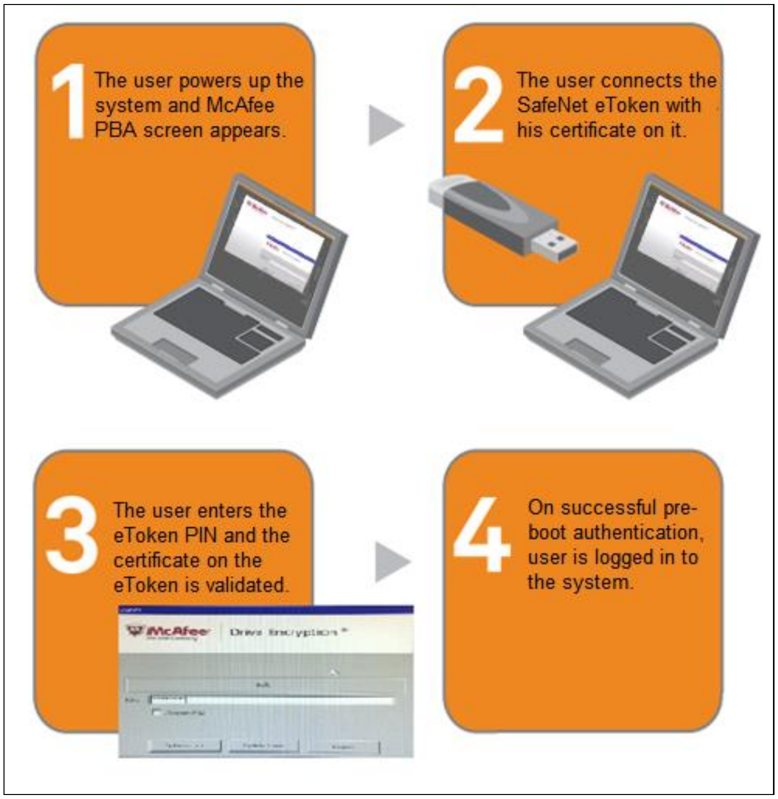
The SafeNet's X.509 certificate-based USB tokens and smartcards provide secure storage for the certificates needed for drive encryption for PC functionality to boot up. If the SafeNet's X.509 certificate-based USB token or smartcard is not inserted in the laptop, or if the certificates are deleted, revoked or expired, the drive encryption for PC software will not boot up and the data on the laptop will stay encrypted and secure.

With this integrated solution, on the pre-boot level, the SafeNet smart card will act as an additional layer of authentication. Whenever the SafeNet smart card is not present, McAfee Drive Encryption will not boot and data will stay encrypted.

This guide describes how to use SafeNet Authentication Client with SafeNet's X.509 certificate-based USB tokens or smartcards to add strong user authentication to McAfee Drive Encryption.

Authentication Flow

The diagram below illustrates the flow of certificate-based authentication during pre-boot:


1
The user powers up the system and McAfee PBA screen appears.
2
The user connects the SafeNet eToken with his certificate on it.
3
The user enters the eToken PIN and the certificate on the eToken is validated.
McAfee
Drive Encryption
4
On successful pre-boot authentication, user is logged in to the system.

1. A user powers up the system. The McAfee pre-boot login screen is displayed.
2. The user connects the SafeNet eToken on which his certificate resides.
3. The user provides the eToken PIN.
4. The system validates the certificate on the SafeNet eToken.

   On successful validation, if single sign-on is configured in the policies, the user is logged in to the system. If single sign-on is not configured in the policies, the Windows login screen is displayed after pre-boot login.

Environment

The integration environment that was used in this document is based on the following software versions:

- SafeNet Authentication Client 8.3 SP1
- McAfee ePolicy Orchestrator 5.1.0 (build 509)
- McAfee Drive Encryption 7.1.1 (minor version 454)

The tokens tested in this integration are as follows:

Token Type	Connection	Integration Type
SafeNet eToken Pro 32K - CardOS 4.2b	USB	PKI Stored Value
SafeNet eToken Pro 64K - CardOS 4.2b	USB	PKI Stored Value
SafeNet eToken Java 72k	USB	PKI Stored Value
SafeNet eToken NG-OTP	USB	PKI Stored Value
SafeNet Ikey 2032	USB	PKI Stored Value
SafeNet eToken 5100	USB	PKI Stored Value
SafeNet eToken 5105	USB	PKI Stored Value
SafeNet eToken 5200	USB	PKI Stored Value
SafeNet eToken 5205	USB	PKI Stored Value
SafeNet eToken 7300 (Standard)	USB	PKI Stored Value

Audience

This document is targeted to system administrators familiar with the McAfee ePolicy Orchestrator 5.1, and who are interested in adding certificate-based authentication (CBA) during pre-boot using SAC.

Solution Prerequisites

To enable SafeNet Authentication Client integrate successfully with McAfee Drive Encryption ensure the following:

- SAC is installed also on the certificate authority from where a certificate will be enrolled on the token.
- A user is created in Active Directory and an appropriate certificate is enrolled for the user on the smart card. The certificate is located on the **Published Certificates** tab within the user's properties in Active Directory.
- A user can log in to the Windows client machine using a certificate on the token prior to disk encryption.
- The Drive Encryption (DE) extensions and software packages are installed in ePolicy Orchestrator (ePO).
- A user must have administrator privileges on the McAfee ePO and must have deployed DE on the clients.
- The LDAP synchronization task is scheduled and run normally between ePO and AD.
- Active Directory, LDAP server, ePO server, and client are up and running and can communicate with each other.

Integration Checklist

To accomplish SAC integration with McAfee Drive Encryption, the following main configuration steps are required:

- Main configuration steps required in McAfee ePolicy Orchestrator:
  a. Assigning a User
  b. Creating a User-Based Policy
  c. Enabling User-Based Policy Enforcement for a User
  d. Associating a Policy with a User
  e. Waking up the Agent on the Client System
- Main configuration steps required in McAfee Drive Encryption:
  a. Installing McAfee® Drive Encryption 7.1.1
  b. Installing SAC 8.3 SP1
  c. Enrolling client certificate on Card Certificate-Based Tokens or smartcard
  d. Checking and Enforcing ePO policies

Configuring McAfee ePolicy Orchestrator

To perform the main configuration settings in McAfee ePolicy Orchestrator, log in to the McAfee ePolicy Orchestrator server with administrator credentials.

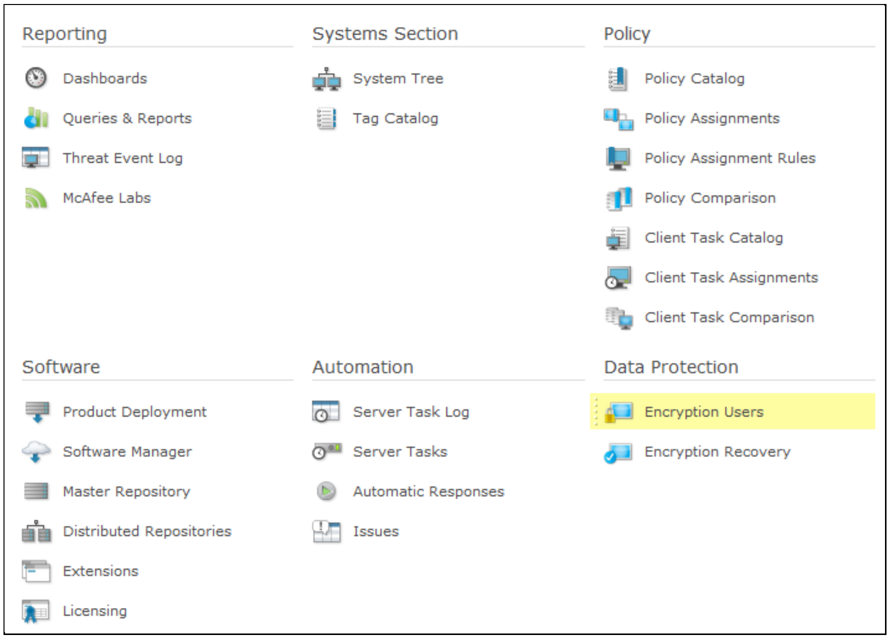
Assigning a User

To activate the Drive Encryption software on a client system, you need to add a user on the McAfee ePO server and enforce the required encryption policies correctly.

The McAfee ePO server allows an administrator to assign users on the drive-encrypted client system for pre-boot authentication.

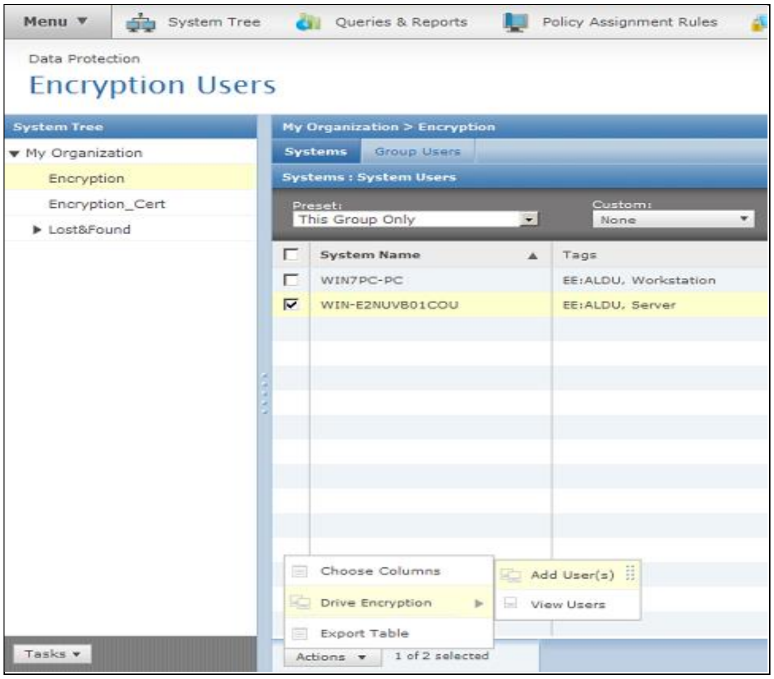
To assign a user:

1. In the McAfee ePolicy Orchestrator main window, click **Menu**.
2. Under **Data Protection**, click **Encryption Users**.



(The screen image above is from McAfee® software. Trademarks are the property of their respective owners.)

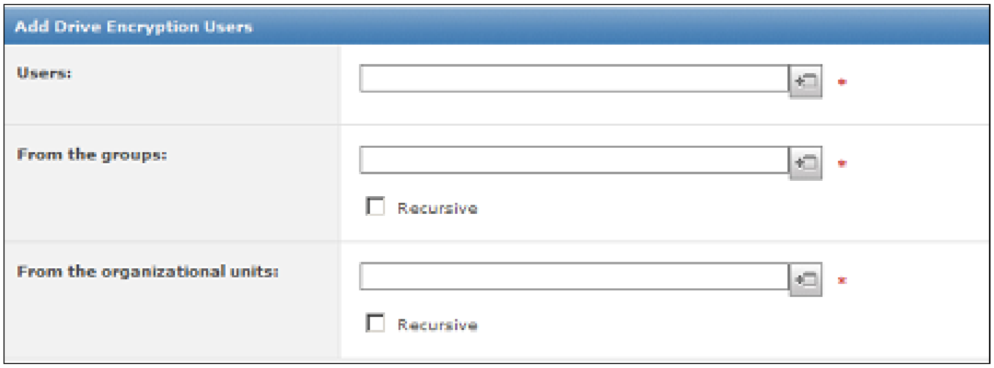
3. In the **Encryption Users** window, do the following:
   a. In the left pane, select a sub-group (for example, **Encryption**).
   b. In the right pane, on the **Systems** tab select the system to which you want to assign users.
   c. Click **Actions > Drive Encryption > Add Users(s)**.



	System Name	Tags
□	WIN7PC-PC	EE:ALDU, Workstation
☑	WIN-E2NUVB01COU	EE:ALDU, Server

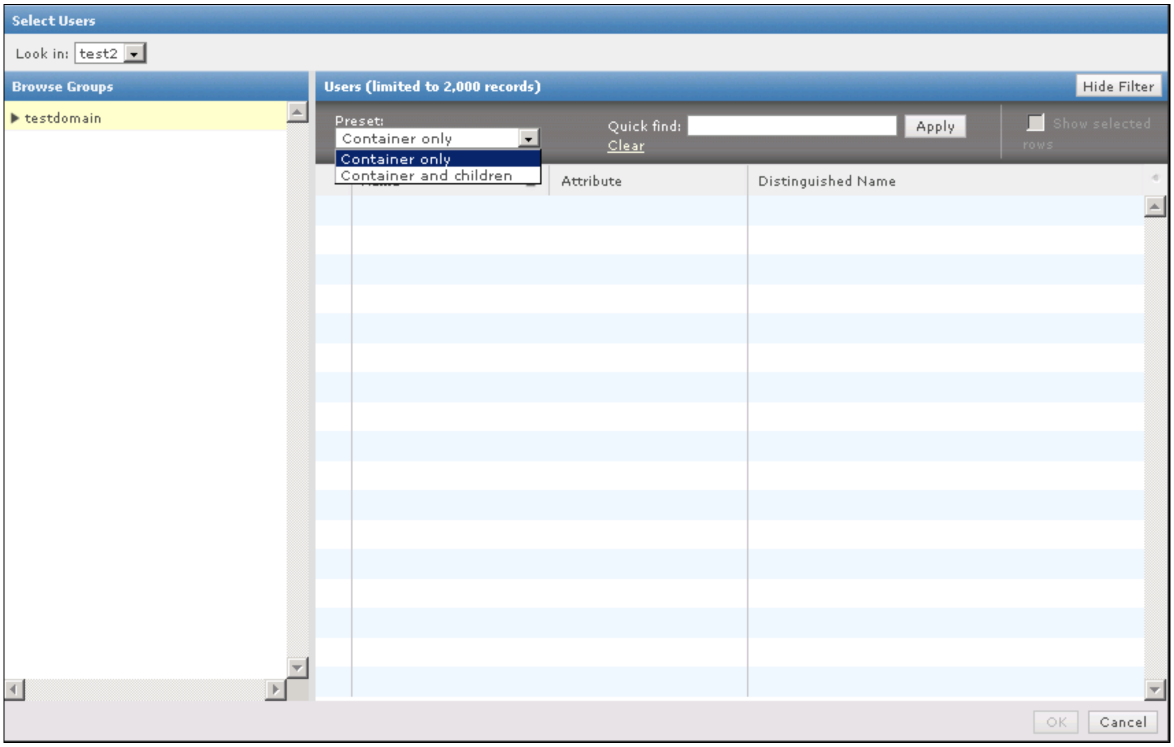
(The screen image above is from McAfee® software. Trademarks are the property of their respective owners.)

4. In the **Add Drive Encryption Users** window, in the **Users** field, click **+** to browse.



(The screen image above is from McAfee® software. Trademarks are the property of their respective owners.)

5. In the **Select Users** window, in the right pane, from the **Preset** list, select **Container and children**. The list of users is displayed in the same window.



(The screen image above is from McAfee® software. Trademarks are the property of their respective owners.)

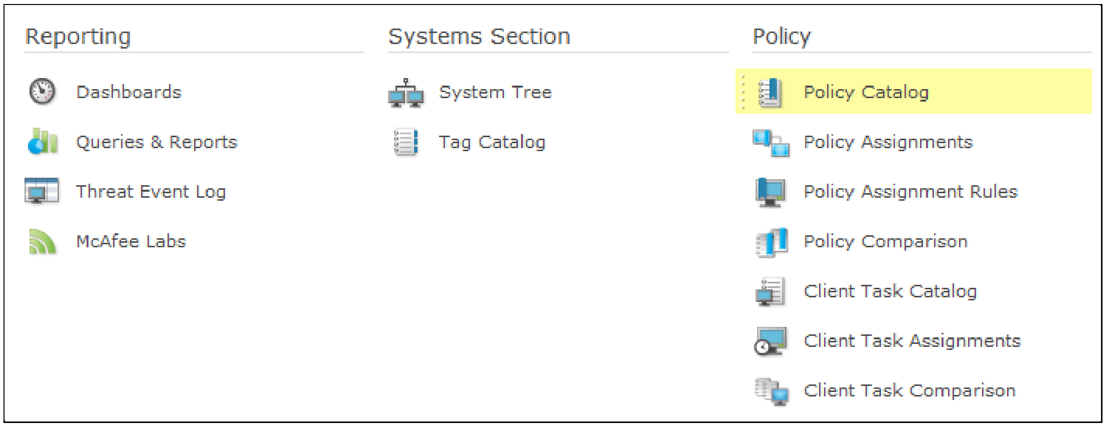
6. Select a user and then click **OK**.

Creating a User-Based Policy

To assign a specific token to a user, create a User-Based Policy (UBP) associated with that token type.

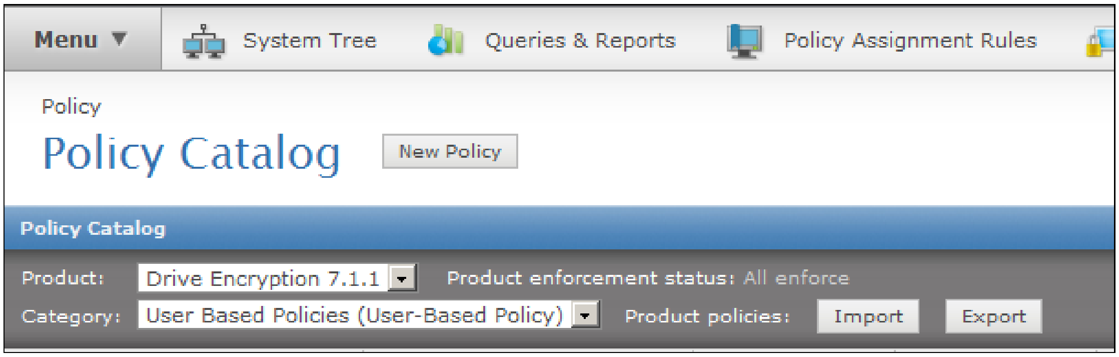
To enable the SafeNet tokens during pre-boot, do the following:

1. In the McAfee ePolicy Orchestrator main window, click **Menu**.
2. Under **Policy**, click **Policy Catalog**.



(The screen image above is from McAfee® software. Trademarks are the property of their respective owners.)

3. In the **Policy Catalog** window, click **New Policy**.

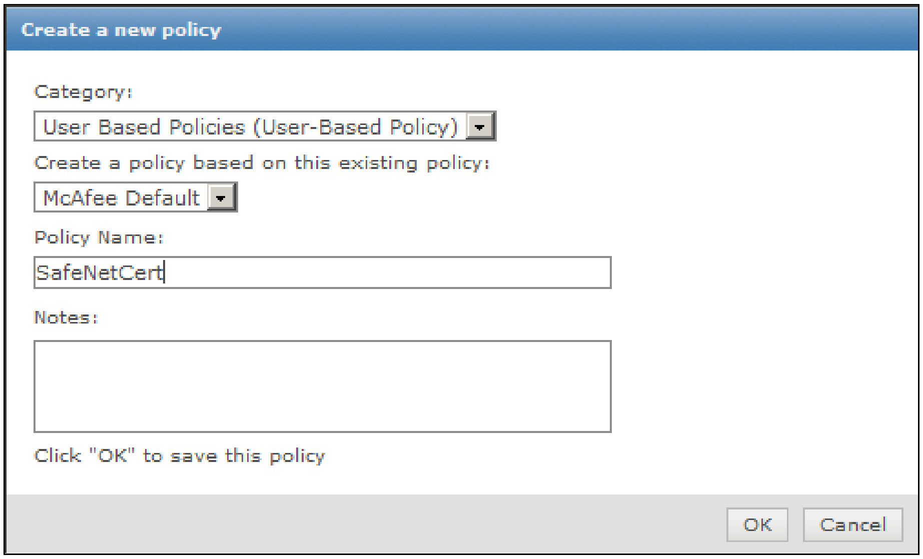


Product: Drive Encryption 7.1.1
Category: User Based Policies (User-Based Policy)

(The screen image above is from McAfee® software. Trademarks are the property of their respective owners.)

4. In the **Create a new policy** window, complete the following fields, and then click **OK**.

Category	Select **User Based Policies**.
Create a policy based on this existing policy	Select **McAfee Default**.
Policy Name	Enter a name for this new policy.



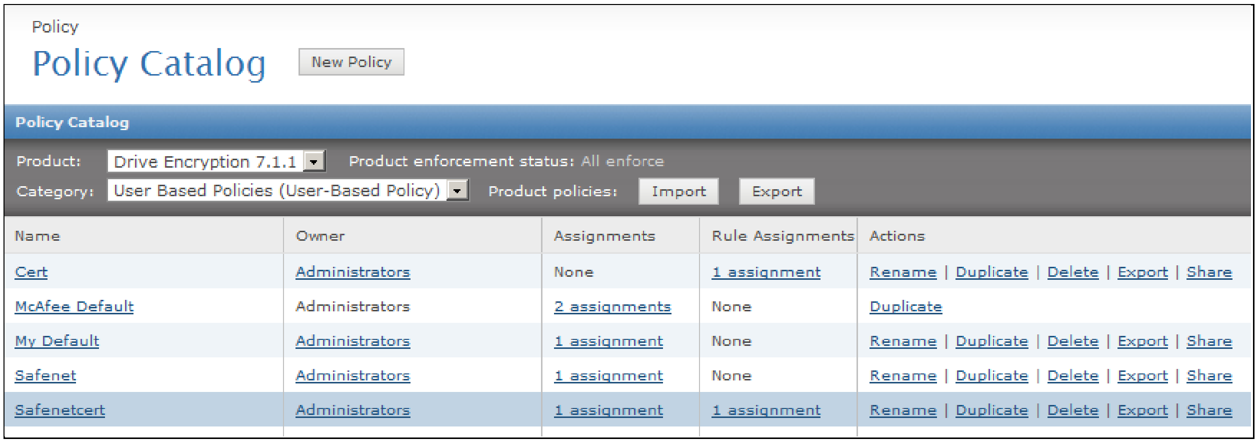
Category: User Based Policies (User-Based Policy)

Create a policy based on this existing policy: McAfee Default

Policy Name: SafeNetCert

(The screen image above is from McAfee® software. Trademarks are the property of their respective owners.)

5. In the **Policy Catalog** window, in the **Name** column, click the newly created policy. The policy details are displayed.



Policy

Policy Catalog

Policy Catalog

Product: Drive Encryption 7.1.1 Product enforcement status: All enforce

Category: User Based Policies (User-Based Policy) Product policies:

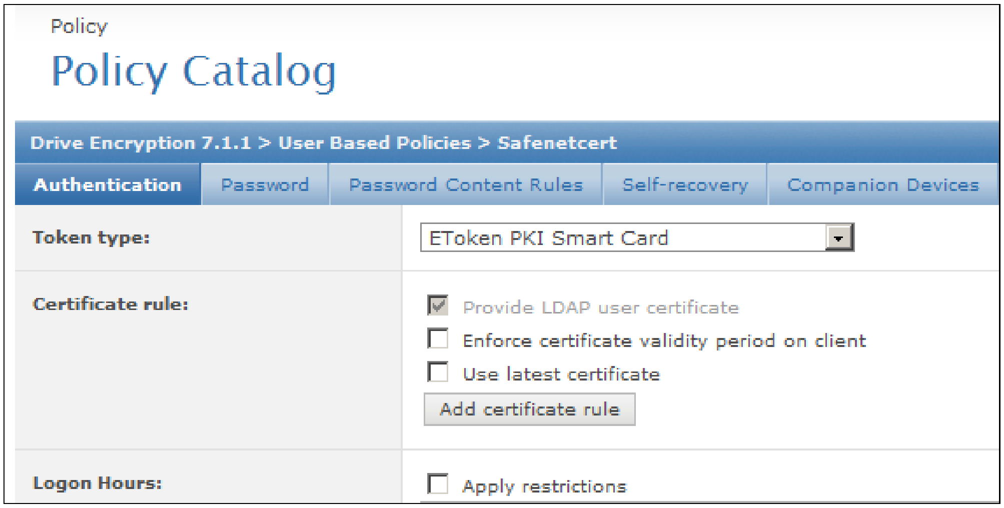
Name	Owner	Assignments	Rule Assignments	Actions
Cert	Administrators	None	1 assignment	Rename | Duplicate | Delete | Export | Share
McAfee Default	Administrators	2 assignments	None	Duplicate
My Default	Administrators	1 assignment	None	Rename | Duplicate | Delete | Export | Share
Safenet	Administrators	1 assignment	None	Rename | Duplicate | Delete | Export | Share
Safenetcert	Administrators	1 assignment	1 assignment	Rename | Duplicate | Delete | Export | Share

(The screen image above is from McAfee® software. Trademarks are the property of their respective owners.)

6. On the **Safenetcert** window, on the **Authentication** tab, in the **Token type** field, select **EToken PKI Smart Card**.

NOTE: In the **Token type** field, the SafeNet tokens **EToken PKI Smart Card** and **EToken Smart Card** are listed. **EToken PKI Smart Card** is for certificate-based authentication at pre-boot.

NOTE: If you are using **Ikey** token for certificate-based authentication at pre-boot, then in the **Token type** field, select **Ikey PKI Smart Card**.



Policy

Policy Catalog

Drive Encryption 7.1.1 > User Based Policies > Safenetcert

Token type: EToken PKI Smart Card

Certificate rule:

☑ Provide LDAP user certificate

□ Enforce certificate validity period on client

□ Use latest certificate

Logon Hours: □ Apply restrictions

(The screen image above is from McAfee® software. Trademarks are the property of their respective owners.)

7. Click **Save**.

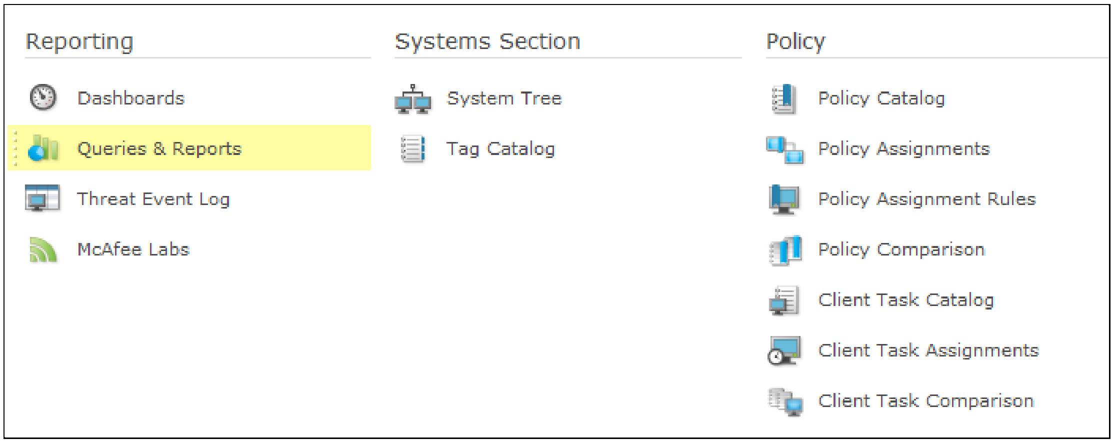
Enabling User-Based Policy Enforcement for a User

All users inherit the default User-Based Policy (UBP) assigned to a system and are prevented from using policy assignment rules. To allow a user to use a policy other than the default user-based policy, enable the UBP enforcement for that user.

To enable UBP enforcement for a user:

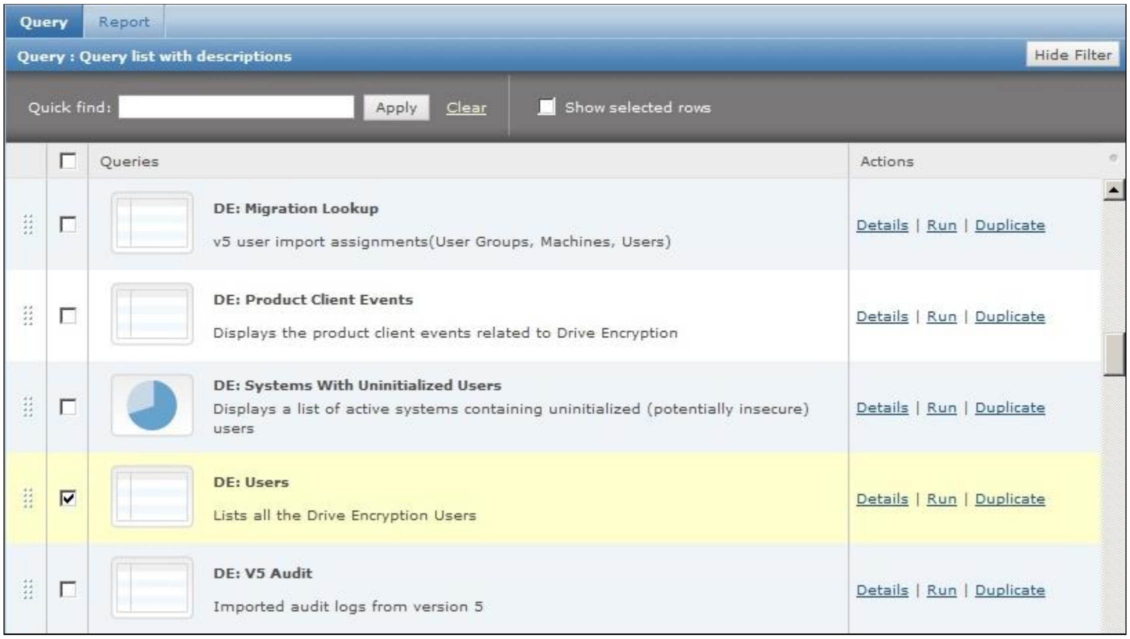
1. In the McAfee ePolicy Orchestrator main window, click **Menu**.

2. Under **Reporting**, click **Queries and Reports**.



(The screen image above is from McAfee® software. Trademarks are the property of their respective owners.)

3. In the **Query** window, to list all drive encryption users, select the **DE: Users** query, and then click the **Run** link on the right in that row.

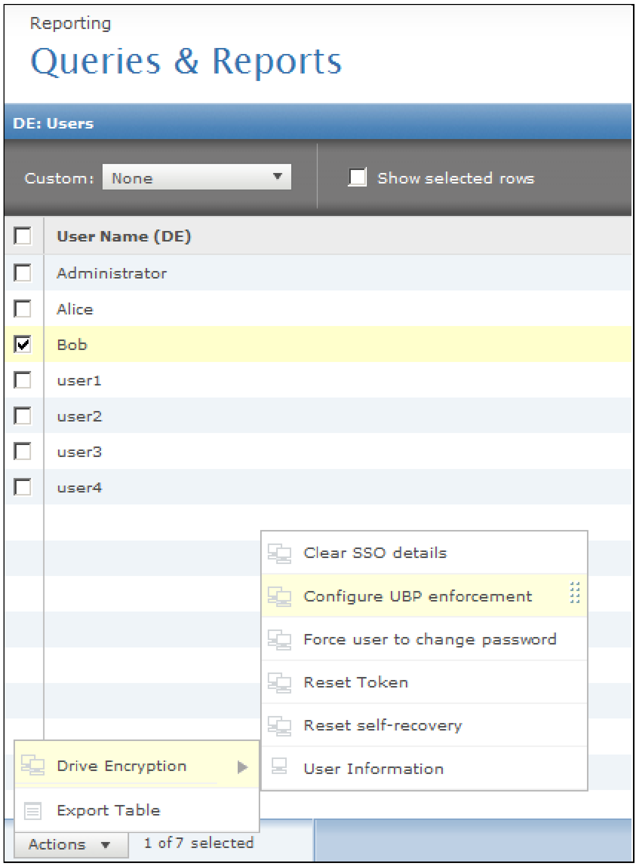


Query : Query list with descriptions

	Queries	Actions
□	**DE: Migration Lookup** v5 user import assignments(User Groups, Machines, Users)	Details | Run | Duplicate
□	**DE: Product Client Events** Displays the product client events related to Drive Encryption	Details | Run | Duplicate
□	**DE: Systems With Uninitialized Users** Displays a list of active systems containing uninitialized (potentially insecure) users	Details | Run | Duplicate
☑	**DE: Users** Lists all the Drive Encryption Users	Details | Run | Duplicate
□	**DE: V5 Audit** Imported audit logs from version 5	Details | Run | Duplicate

(The screen image above is from McAfee® software. Trademarks are the property of their respective owners.)

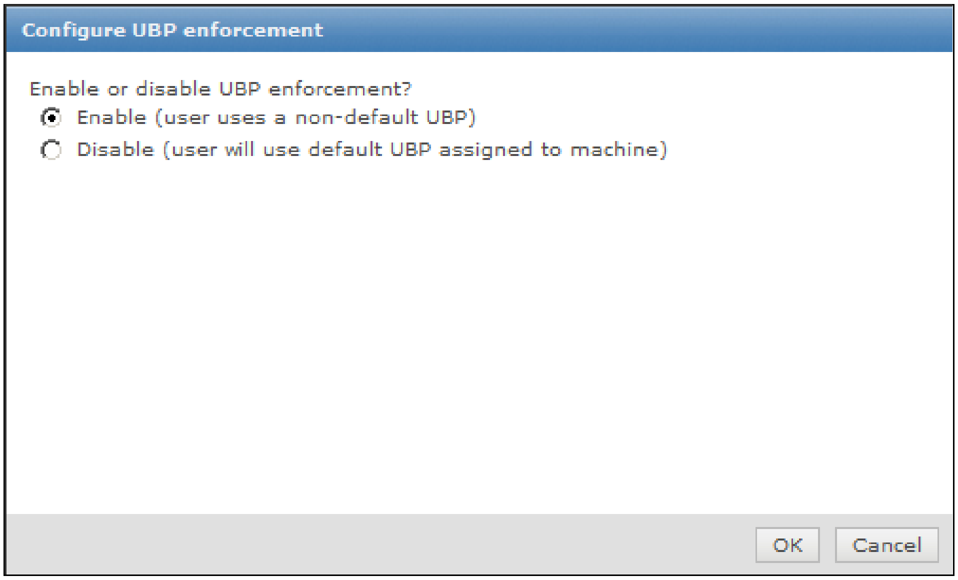
4. In the **DE: Users** window, select the users for which you want to enforce the policy. Next, click **Actions > Drive Encryption > Configure UBP enforcement.**



□	User Name (DE)
□	Administrator
□	Alice
☑	Bob
□	user1
□	user2
□	user3
□	user4

(The screen image above is from McAfee® software. Trademarks are the property of their respective owners.)

5. In the **Configure UBP enforcement** window, select **Enable** and then click **OK**.



Enable or disable UBP enforcement?

● Enable (user uses a non-default UBP)

○ Disable (user will use default UBP assigned to machine)

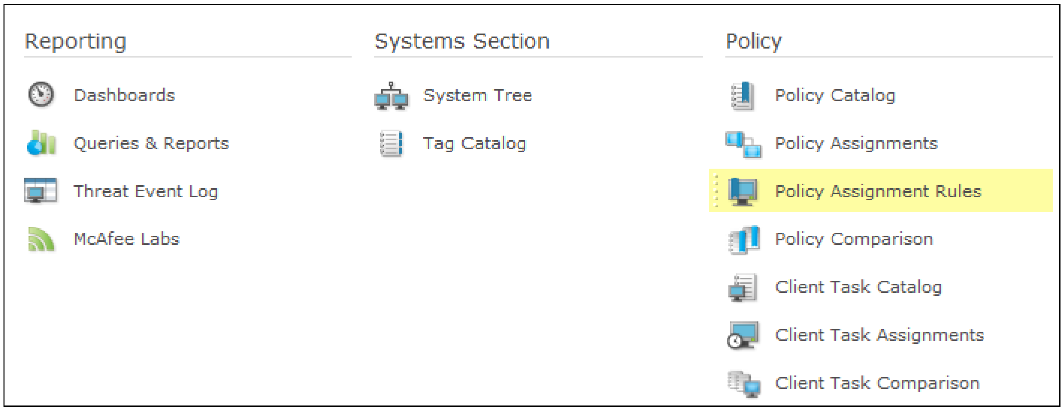
(The screen image above is from McAfee® software. Trademarks are the property of their respective owners.)

Associating a Policy with a User

When a user is assigned access to a system, and a user-based policy exists for the **EToken PKI Smart Card** token type, ensure that user-based policies are enforced for that user.

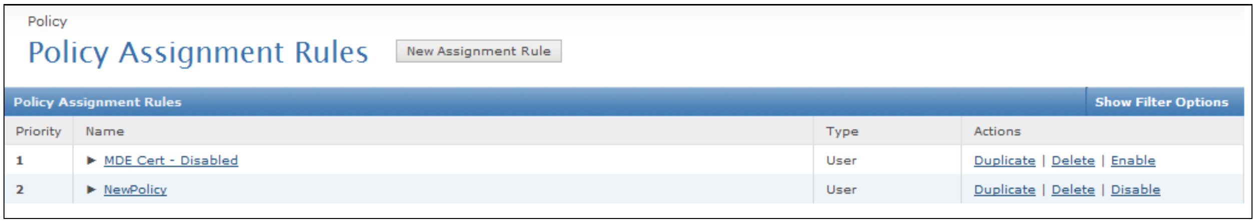
Define the policy assignment rule by specifying policies that are applied to users and the criteria on which the rule is applied.

1. In the McAfee ePolicy Orchestrator main window, click **Menu**.
2. Under **Policy**, click **Policy Assignment Rules**.



(The screen image above is from McAfee® software. Trademarks are the property of their respective owners.)

3. In the **Policy Assignment Rules** window, click **New Assignment Rule**.



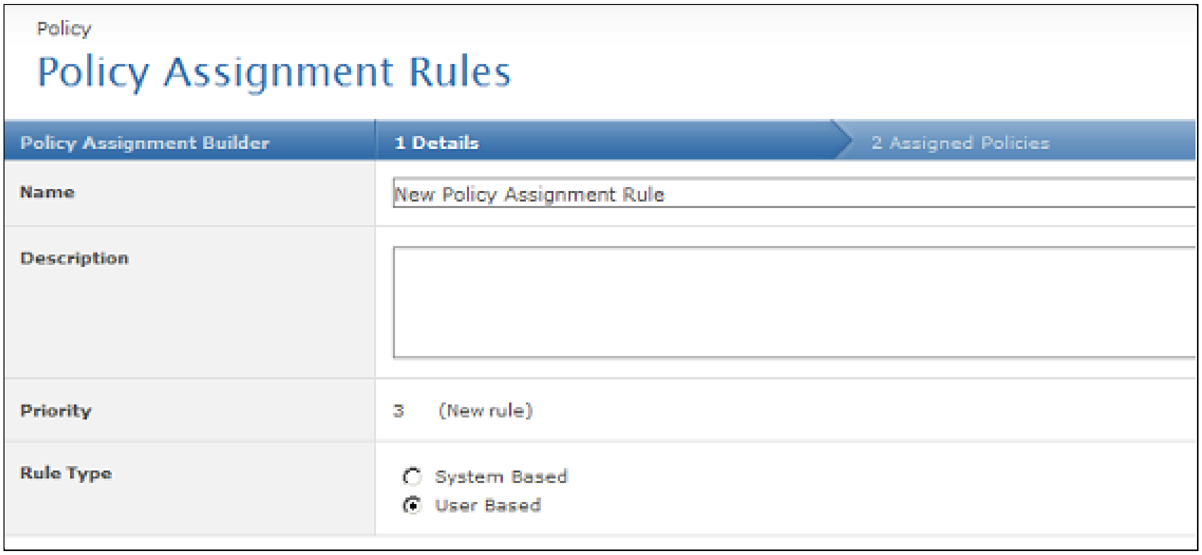
Policy Assignment Rules

Priority	Name	Type	Actions
1	▶ MDE Cert - Disabled	User	Duplicate | Delete | Enable
2	▶ NewPolicy	User	Duplicate | Delete | Disable

(The screen image above is from McAfee® software. Trademarks are the property of their respective owners.)

4. On the **Details** tab, complete the policy details as specified below, and then click **Next**.

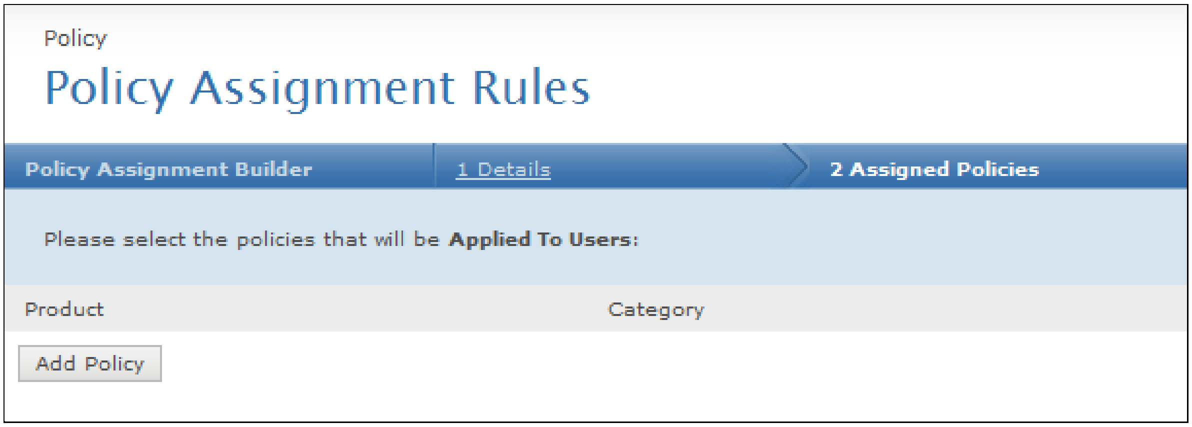
Name	Enter a name for the policy assignment rule.
Description	Enter a description of the policy assignment rule.
Rule Type	Select **User Based**.



Name	New Policy Assignment Rule
Description	
Priority	3 (New rule)
Rule Type	○ System Based ● User Based

(The screen image above is from McAfee® software. Trademarks are the property of their respective owners.)

5. On the **Assigned Policies** tab, click **Add Policy**.

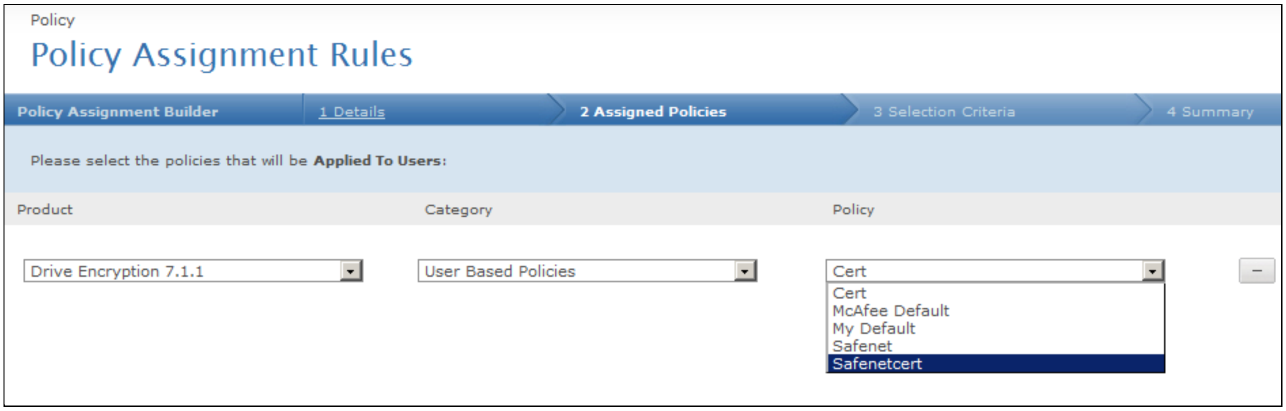


Please select the policies that will be **Applied To Users:**

(The screen image above is from McAfee® software. Trademarks are the property of their respective owners.)

6. On the **Assigned Policies** tab, complete the following fields, and then click **Next**.

Product	Select **Drive Encryption 7.1.1**.
Category	Select **User Based Policies**.
Policy	Select a user-based policy; for example, **Safenetcert**.



Policy

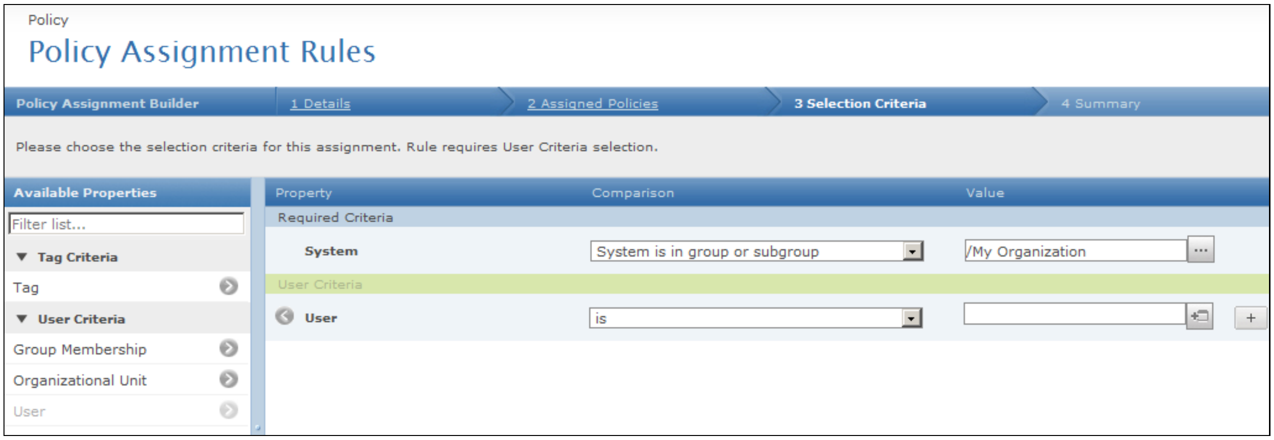
Policy Assignment Rules

Please select the policies that will be **Applied To Users**:

Product	Category	Policy
Drive Encryption 7.1.1	User Based Policies	Cert

(The screen image above is from McAfee® software. Trademarks are the property of their respective owners.)

7. On the **Selection Criteria** tab, specify the criteria for **System** and **User**, and then click **Next**.



Policy

Policy Assignment Rules

Please choose the selection criteria for this assignment. Rule requires User Criteria selection.

Property	Comparison	Value
Required Criteria		
System	System is in group or subgroup	/My Organization
User Criteria		
User	is	

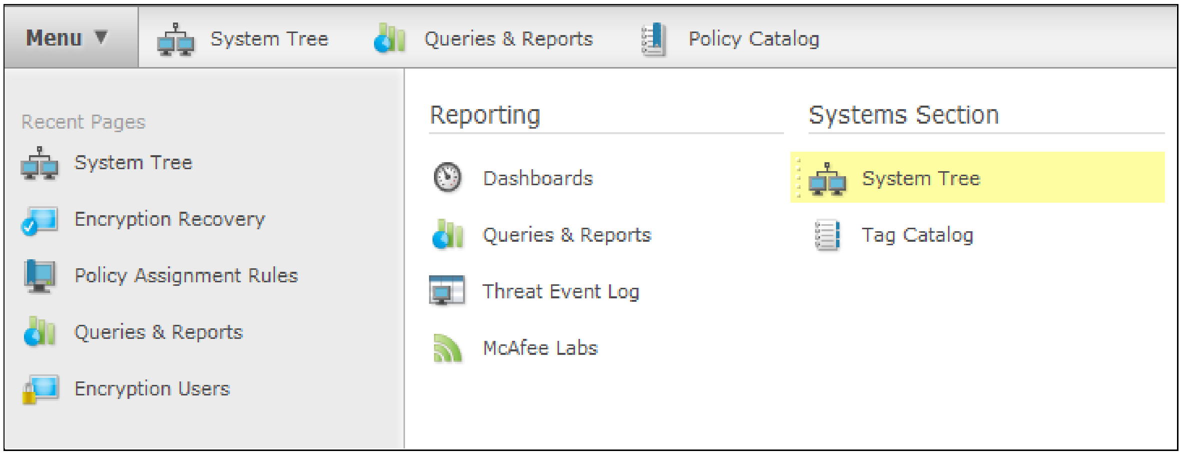
(The screen image above is from McAfee® software. Trademarks are the property of their respective owners.)

8. In the **Summary** window, review the details, and then click **Save**.

Waking up the Agent on the Client System

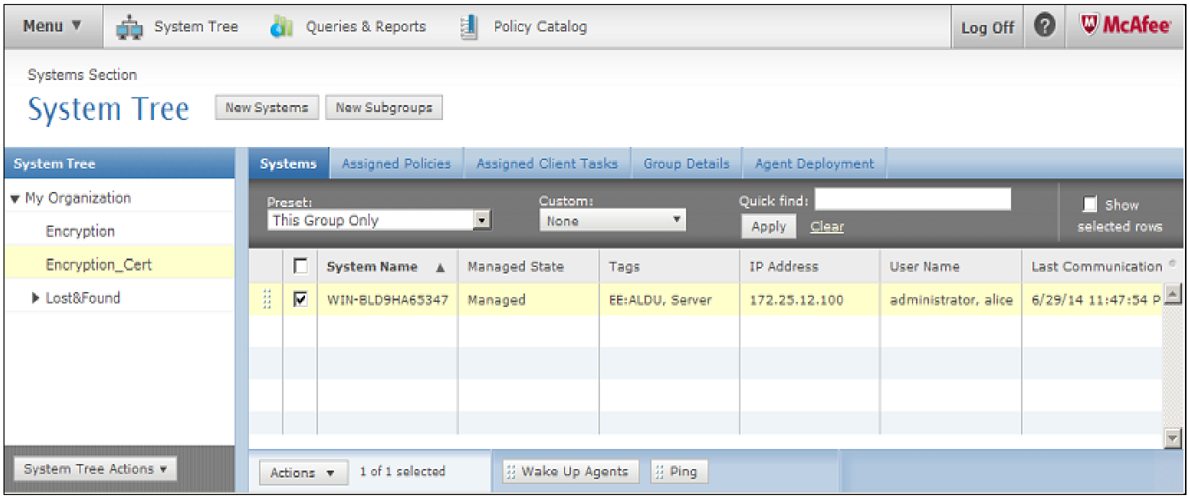
The client computer gets the policy update whenever it connects to the McAfee ePO server during the next agent-server communication interval (ASCI). The policy update can be scheduled or forced. The Agent Wake-Up Call forces the policy update on the client system.

1. In the McAfee ePolicy Orchestrator main window, click **Menu**.
2. Under **Systems Section**, click **System Tree**.



(The screen image above is from McAfee® software. Trademarks are the property of their respective owners.)

3. In the **System Tree** window, in the right pane, on the **Systems** tab, select the client system and then click **Wake Up Agents**.

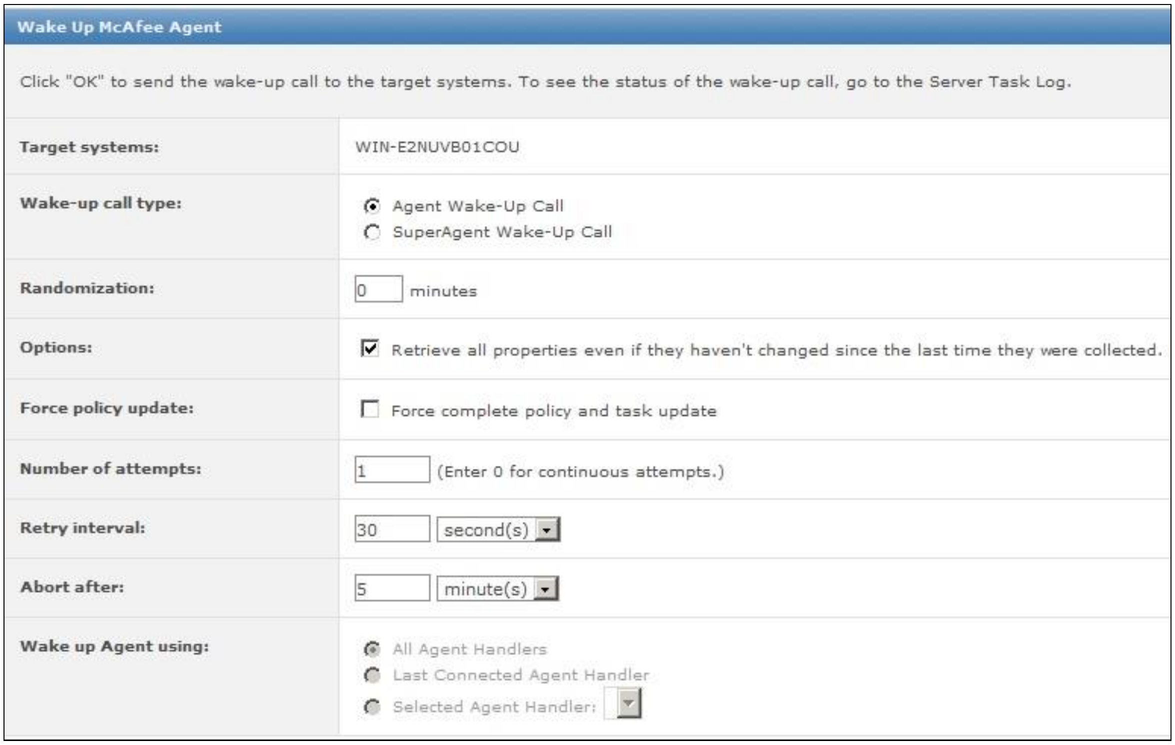


Preset: This Group Only
Custom: None

	System Name ▲	Managed State	Tags	IP Address	User Name	Last Communication
☑	WIN-BLD9HA65347	Managed	EE:ALDU, Server	172.25.12.100	administrator, alice	6/29/14 11:47:54 P

(The screen image above is from McAfee® software. Trademarks are the property of their respective owners.)

4. In the **Wake Up McAfee Agent** window, select **Force complete policy and task update** and then click **OK**.



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.

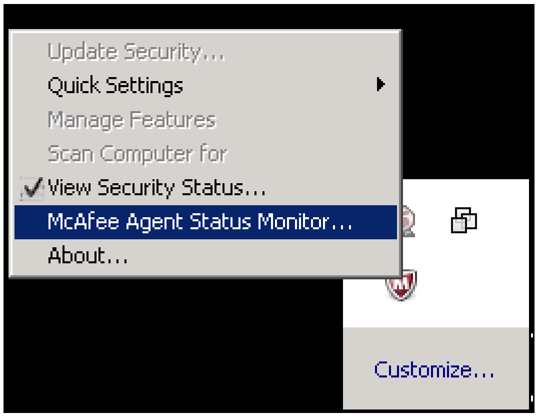
Target systems:	WIN-E2NUVB01COU
Wake-up call type:	● Agent Wake-Up Call ○ SuperAgent Wake-Up Call
Randomization:	0 minutes
Options:	☑ Retrieve all properties even if they haven't changed since the last time they were collected.
Force policy update:	□ Force complete policy and task update
Number of attempts:	1 (Enter 0 for continuous attempts.)
Retry interval:	30 second(s)
Abort after:	5 minute(s)
Wake up Agent using:	● All Agent Handlers ○ Last Connected Agent Handler ○ Selected Agent Handler:

(The screen image above is from McAfee® software. Trademarks are the property of their respective owners.)

Configurations on the Client Machine

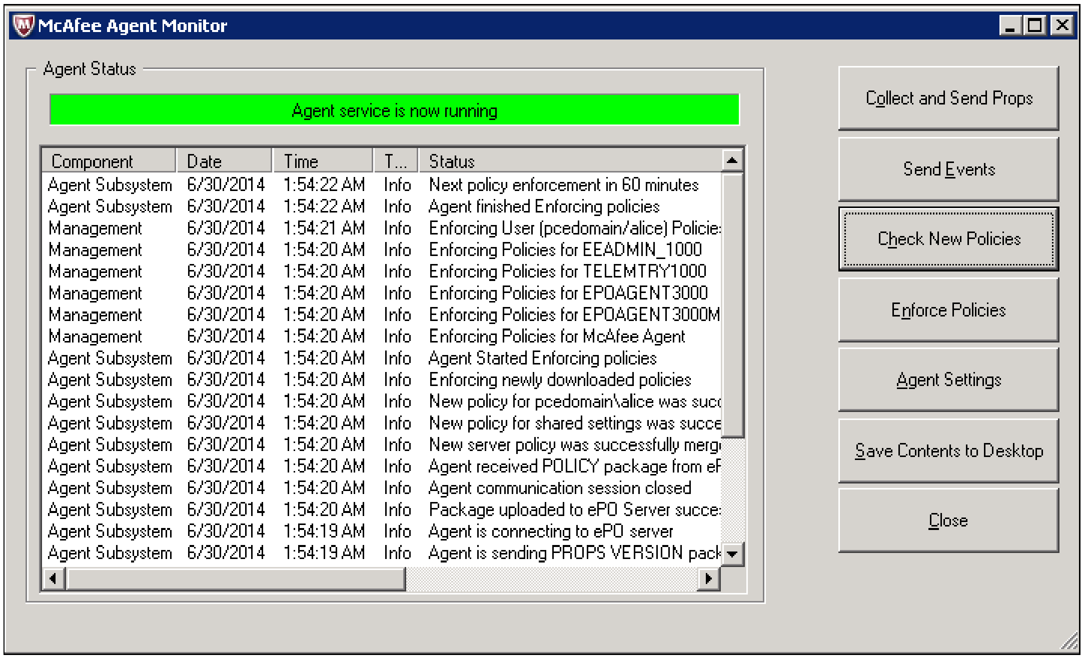
On the client machine, use the McAfee Agent user interface to check and enforce new policies.

1. On the taskbar, right-click the McAfee tray icon.
2. Click **McAfee Agent Status Monitor**.



(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

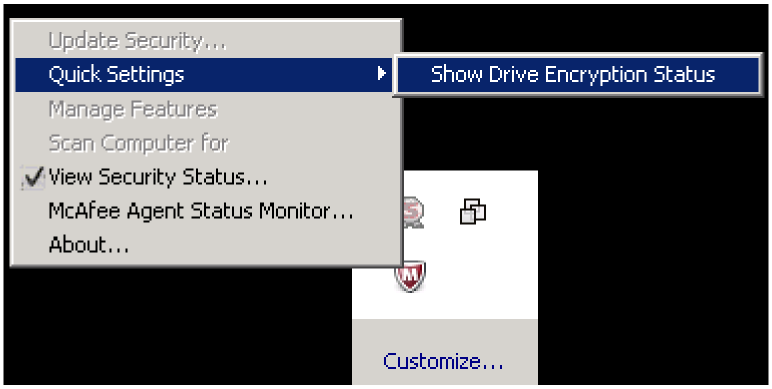
3. In the **McAfee Agent Monitor** window, do the following:
   a. Click **Check New Policies**.
   b. Click **Enforce Policies**.
   c. Click **Close**.



Component	Date	Time	T...	Status
Agent Subsystem	6/30/2014	1:54:22 AM	Info	Next policy enforcement in 60 minutes
Agent Subsystem	6/30/2014	1:54:22 AM	Info	Agent finished Enforcing policies
Management	6/30/2014	1:54:21 AM	Info	Enforcing User (pcedomain/alice) Policie:
Management	6/30/2014	1:54:20 AM	Info	Enforcing Policies for EEADMIN_1000
Management	6/30/2014	1:54:20 AM	Info	Enforcing Policies for TELEMTRY1000
Management	6/30/2014	1:54:20 AM	Info	Enforcing Policies for EPOAGENT3000
Management	6/30/2014	1:54:20 AM	Info	Enforcing Policies for EPOAGENT3000M
Management	6/30/2014	1:54:20 AM	Info	Enforcing Policies for McAfee Agent
Agent Subsystem	6/30/2014	1:54:20 AM	Info	Agent Started Enforcing policies
Agent Subsystem	6/30/2014	1:54:20 AM	Info	Enforcing newly downloaded policies
Agent Subsystem	6/30/2014	1:54:20 AM	Info	New policy for pcedomain\alice was succ
Agent Subsystem	6/30/2014	1:54:20 AM	Info	New policy for shared settings was succe
Agent Subsystem	6/30/2014	1:54:20 AM	Info	New server policy was successfully merg
Agent Subsystem	6/30/2014	1:54:20 AM	Info	Agent received POLICY package from eP
Agent Subsystem	6/30/2014	1:54:20 AM	Info	Agent communication session closed
Agent Subsystem	6/30/2014	1:54:20 AM	Info	Package uploaded to ePO Server succe:
Agent Subsystem	6/30/2014	1:54:19 AM	Info	Agent is connecting to ePO server
Agent Subsystem	6/30/2014	1:54:19 AM	Info	Agent is sending PROPS VERSION pack

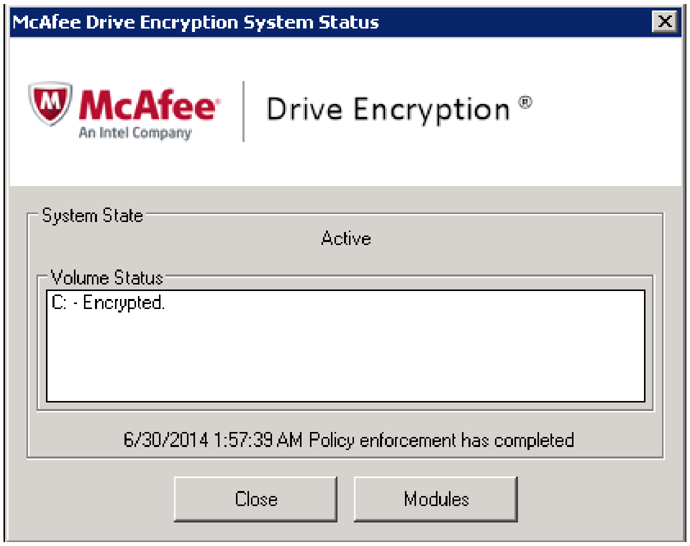
(The screen image above is from McAfee® software. Trademarks are the property of their respective owners.)

4. On the taskbar, right-click the McAfee tray icon and then click **Quick Settings > Show Drive Encryption Status**.



(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

5. In the **McAfee Drive Encryption System Status** window, wait until the policy enforcement process completes and then click **Close**.



System State

Active

Volume Status

C: - Encrypted.

6/30/2014 1:57:39 AM Policy enforcement has completed

(The screen image above is from McAfee® software. Trademarks are the property of their respective owners.)

6. Restart the client machine.

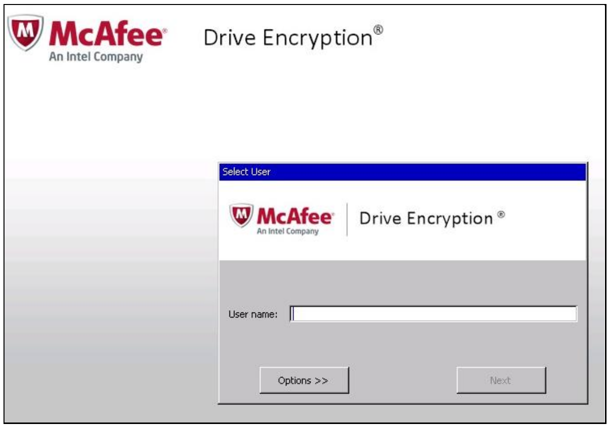
Running the Solution

When the client machine powers up, the system prompts the user to authenticate using EEPC pre-boot application. Ensure that the token (with the installed client certificate) is inserted either before system is powered up or before EEPC prompts for user authentication.

Pre-boot can successfully unlock your system when you present the appropriate smart card (that matches the certificate information found in AD) and the correct PIN. During the first pre-boot after activation, initialize your account with the default password (12345) and enroll for self- recovery (if enabled in the policy).

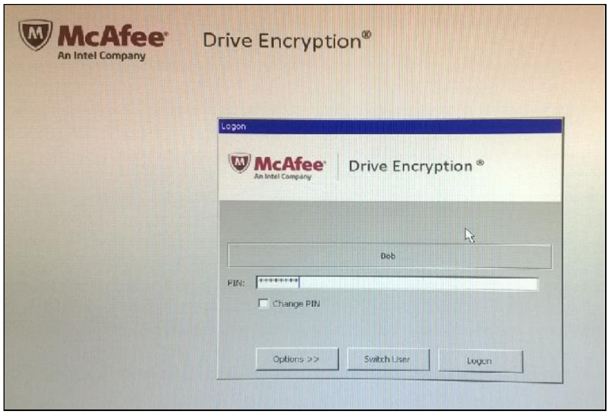
Solution Steps:

1. The user powers up the system.
2. Insert the token (with the certificate of the user) into the client machine. The McAfee PBA screen appears.
3. Enter your **user name** and then click **Next**.



(The screen image above is from McAfee® software. Trademarks are the property of their respective owners.)

4. Enter the **PIN** and then click **Logon**.



Bob

PIN: ********

(The screen image above is from McAfee® software. Trademarks are the property of their respective owners.)

If the PIN is correct, the user is authenticated and the system starts Windows. The token is successfully assigned to the user and can be used for authentication.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Table 1: Support Contacts

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.	