SafeNet Authentication Client

Integration Guide

Using SafeNet Authentication Client CBA for McAfee Drive Encryption

gemalto
security to be free

Document Number: 007-013791-001, Rev. A

Release Date: June 2017

Contents

Third-Party Software Acknowledgement

This document is intended to help users of Gemalto 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.

Description

SafeNet Authentication Client (SAC) is a public key infrastructure (PKI) middleware that provides a secure method for exchanging information based on public key cryptography, enabling trusted third-party verification of user identities. SAC enables the implementation of strong two-factor authentication using standard certificates, as well as encryption and digital signing of data. The SAC generic integration with CAPI, CNG, and PKCS#11 security interfaces enables out-of-the-box interoperability with a variety of security applications, offering security for web access, network logon, email, and data. PKI keys and certificates can be created, stored, and used securely with the hardware or software tokens.

Drive encryption, also referred to as full disk encryption, is encryption software that helps protect data on Microsoft Windows tablets, laptops, and desktop PCs to prevent the loss of sensitive data, especially from lost or stolen equipment. It is designed to make all data on a system drive unintelligible to unauthorized persons, which in turn helps meet compliance requirements.

Drive encryption is compatible with traditional hard drives (spinning media AKA HDD), solid-state drives (SSD), and self-encrypting drives (SED and OPAL). Drive encryption is a software component available in three McAfee data and endpoint protection suites, and is managed through the McAfee ePolicy Orchestrator (McAfee ePO) management console.

An effective strong authentication solution must be able to address data breaches on the rise 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 interoperable with McAfee Drive Encryption, providing a 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, reduced operational costs, and improved compliance by adding smart card-based strong user authentication to McAfee Drive Encryption.

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

The Gemalto's X.509 certificate-based USB tokens and smart cards provide secure storage for the certificates needed for endpoint encryption for McAfee Drive Encryption functionality to boot up. If Gemalto's X.509 certificate-based USB token or smart card is not inserted in the client machine, or if the certificates are deleted, revoked, or expired, the McAfee Drive Encryption software will not boot up and the data on the laptop will stay encrypted and secure.

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to McAfee Drive Encryption using Gemalto tokens or smart cards.

It is assumed that the McAfee Drive Encryption environment is already configured and working with static passwords prior to implementing Gemalto multi-factor authentication.

McAfee Drive Encryption can be configured to support multi-factor authentication in several modes. CBA will be used for the purpose of working with Gemalto products.

Applicability

The information in this document applies to:

- **SafeNet Authentication Client (SAC) Typical installation mode -** SafeNet Authentication Client is public key infrastructure (PKI) middleware that manages Gemalto's tokens and smart cards.
- **SafeNet Authentication Client (SAC) IDGo800 Compatible mode** - IDGo800 Minidriver based package, uses Microsoft Smart Card Base Cryptographic Provider to manage Gemalto IDPrime MD smart cards.

For more details about different SAC installation modes, please refer to Customization section in the *SafeNet Authentication Client Administrator Guide*.

- **McAfee Drive Encryption**

Environment

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

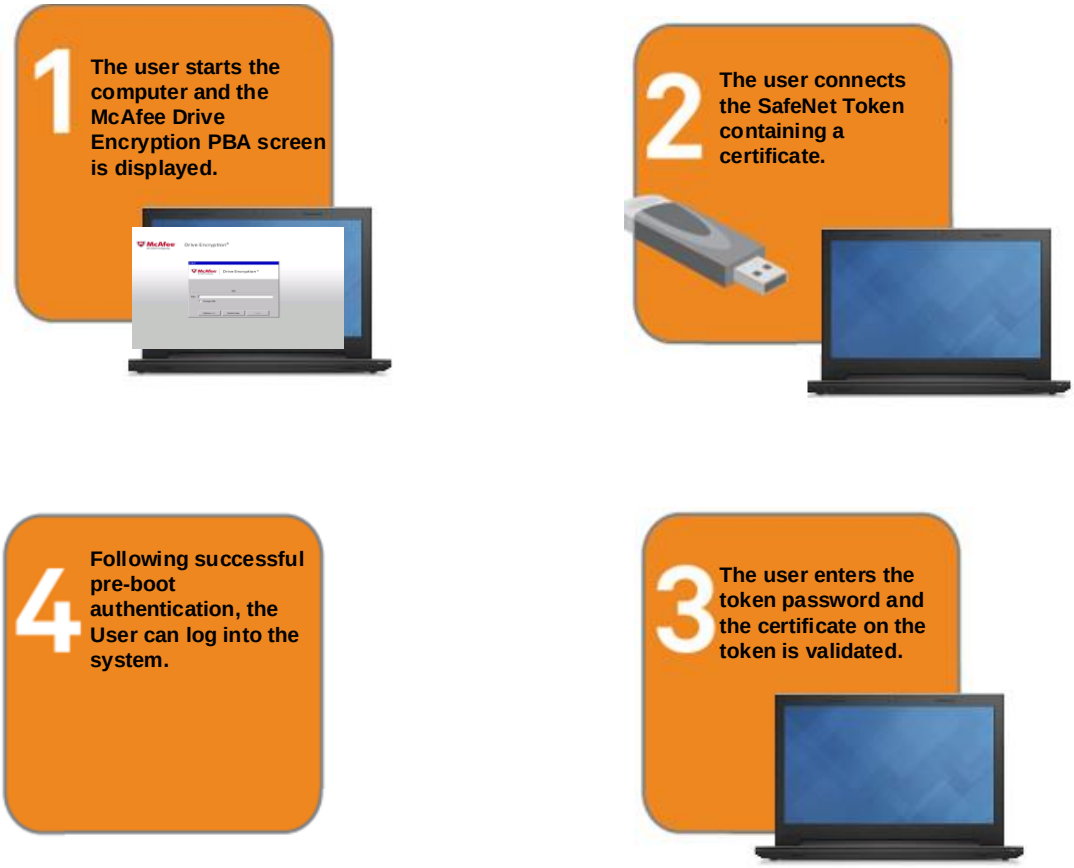
- **SafeNet Authentication Client (SAC)** - 10.3
- **McAfee Drive Encryption** - 7.1.2
- **McAfee ePolicy Orchestrator** - 5.3

Audience

This document is intended for system administrators who are familiar with McAfee Drive Encryption, and are interested in adding multi-factor authentication capabilities during pre-boot using SafeNet tokens.

Pre-Boot Authentication Flow

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



NOTE: Following successful pre-boot validation, if single sign-on is configured in the McAfee Drive Encryption policies, the user is logged into the system. If single sign-on is not configured in the McAfee Drive Encryption policies, the Windows login screen is displayed after pre-boot authentication.

Prerequisites

To enable users to perform pre-boot authentication with McAfee Drive Encryption using Gemalto tokens and smart cards, ensure the following:

- Users can authenticate through pre-boot from the McAfee Drive Encryption environment with a static password before configuring the McAfee Drive Encryption to use Gemalto tokens and smart cards.
- If SafeNet Authentication Manager (SAM) is used to manage the tokens, Token Policy Object (TPO) should be configured with MS CA connector. For further details, refer to the section “Connector for Microsoft CA” in the *SafeNet Authentication Manager Administrator’s Guide*.
- Users have a Gemalto token or smart card with a valid certificate enrolled.
- To use CBA, the Microsoft Enterprise Certificate Authority must be installed and configured. Any CA can be used. In this guide, integration is demonstrated using Microsoft CA.
- SafeNet Authentication Client 10.3 must be installed on all client machines.

Supported Tokens and Smart Cards in SafeNet Authentication Client

SafeNet Authentication Client 10.3 supports the following tokens and smart cards with McAfee Drive Encryption:

Certificate-based USB tokens

- SafeNet eToken 5110 GA

Smart Cards

- Gemalto IDPrime MD 830 L2

Configuring McAfee Drive Encryption

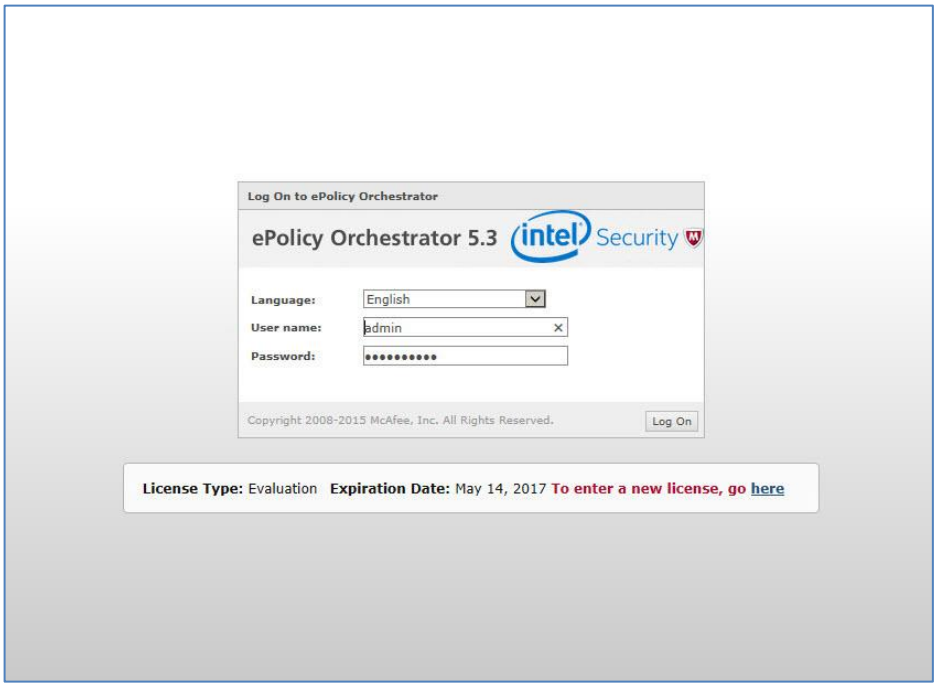
In order to deploy and configure the McAfee Drive Encryption on the client machine, the ePolicy Orchestrator server must be installed.

This document assumes the following:

- McAfee ePolicy Orchestrator is installed.
- The McAfee agent is deployed on client machines.
- Drive Encryption policy is deployed on client machines, and is configured with username and password authentication.

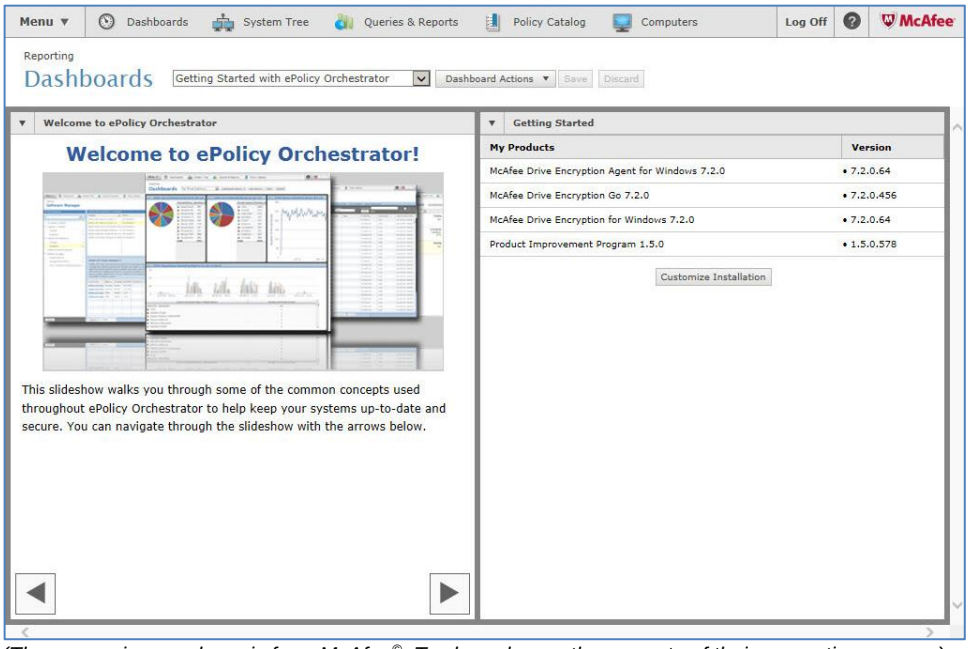
Creating User Based Policy

1. Open the **ePolicy Orchestrator** Login page.



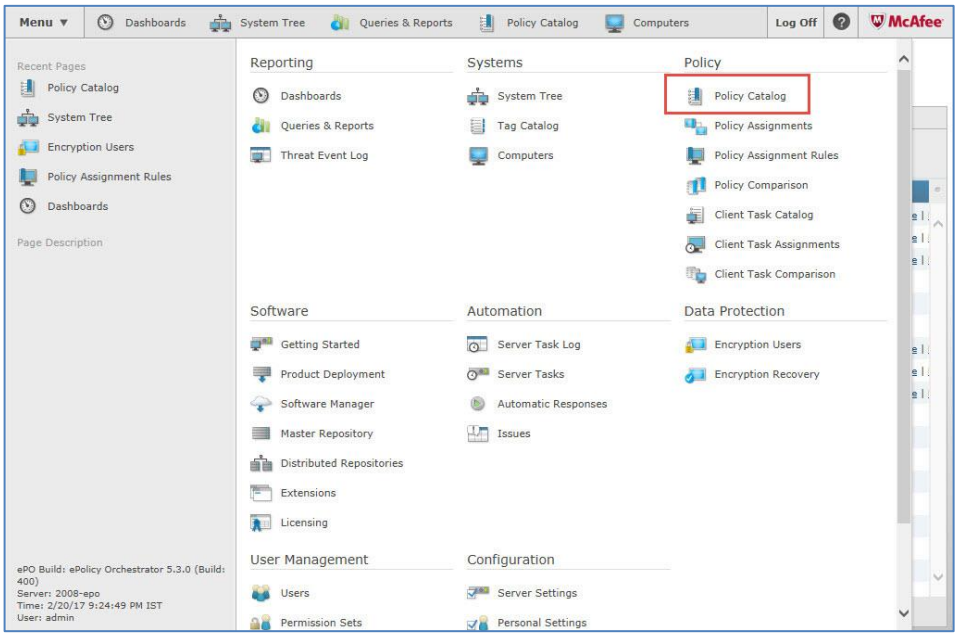
(The screen image above is from McAfee©. Trademarks are the property of their respective owners.)

2. Login to the admin console.



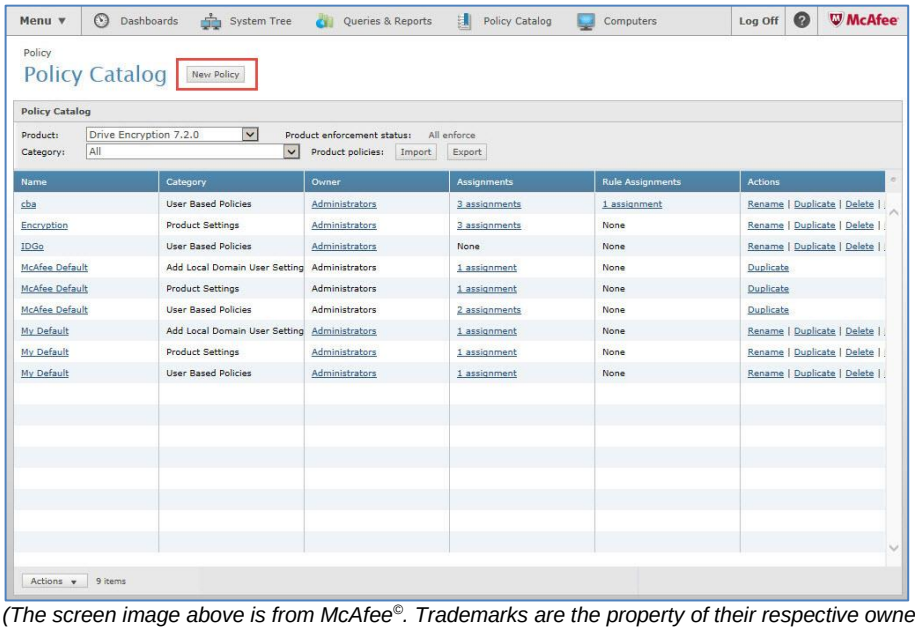
(The screen image above is from McAfee©. Trademarks are the property of their respective owners.)

3. Select **Menu > Policy > Policy Catalog**.



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

4. Click **New Policy**

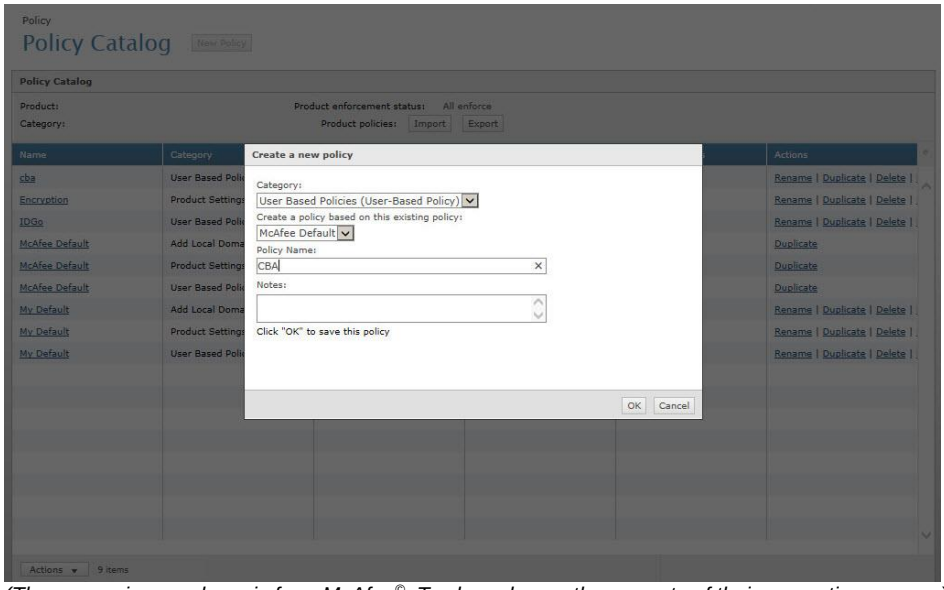


(The screen image above is from McAfee©. Trademarks are the property of their respective owners.)

The **Create a new policy** window opens.

5. Enter the fields as follows:

Field	Description
Category	Select **User Based Policies (User-Based Policy).**
Create a policy based on this existing policy	Select a policy (Default policy is "**MacAfee Default**")
Policy Name	Enter a name for the policy



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

6. Click **OK.**

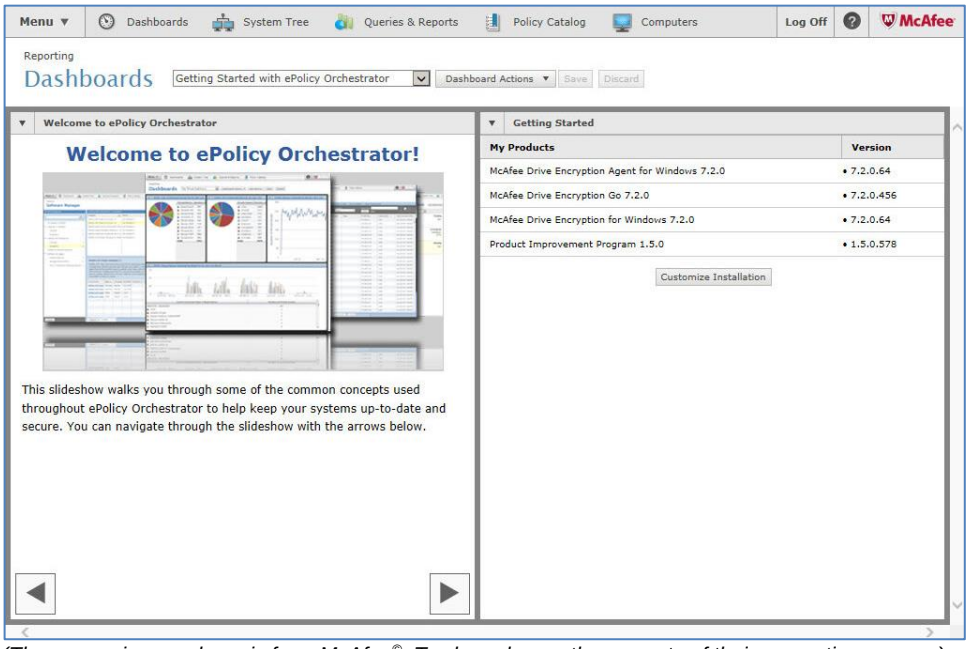
   The new policy has been added to the Policy Catalog.

Configuring CBA Policy

1. Open the **ePolicy Orchestrator** Login page.

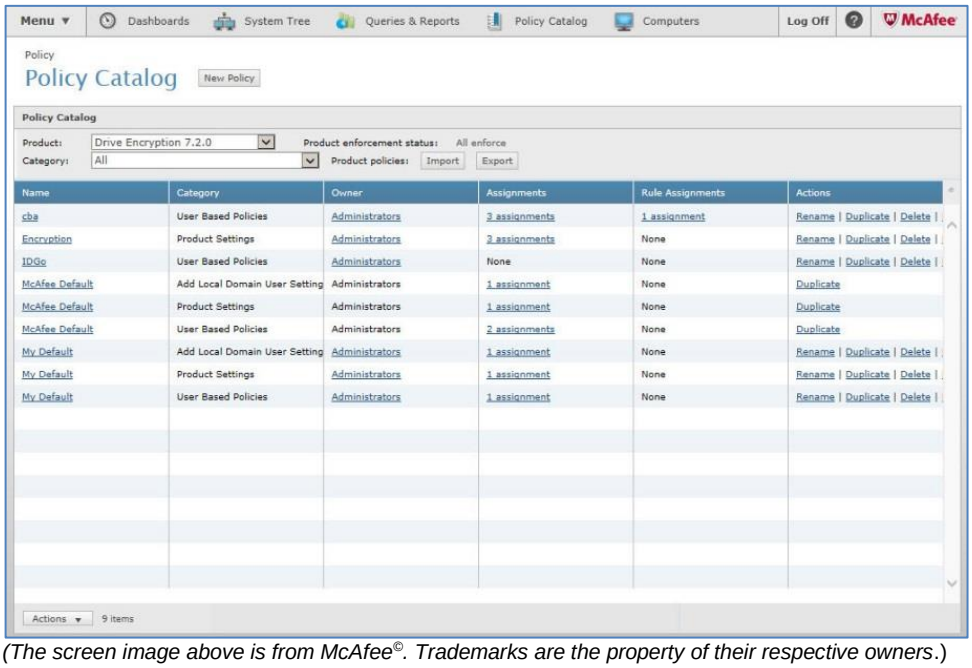
(The screen image above is from McAfee©. Trademarks are the property of their respective owners.)

2. Login to the admin console.



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

3. Select **Menu > Policy >Policy Catalog.**



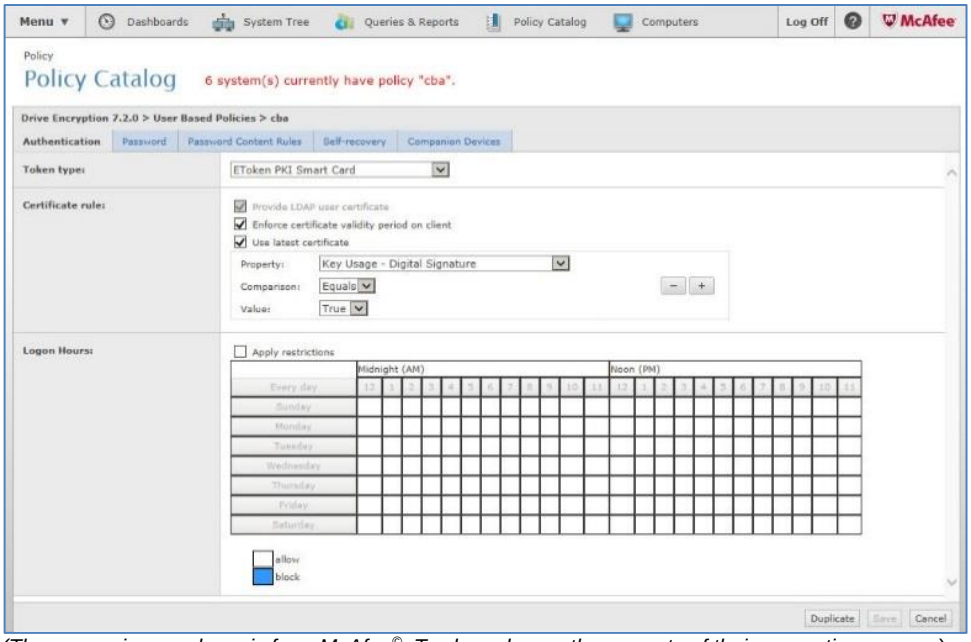
(The screen image above is from McAfee©. Trademarks are the property of their respective owners.)

4. Click the policy you created in the previous section.

   The **Policy** window opens.

5. In the **Authentication** tab, configure the following:

Field	Description
Token type	Select one of the following: • **EToken PKI Smart Card** • **IDPrime MD PKI Smart Card**
Property	Select **Key Usage – Digital Signature**
Comparison	Select **Equals**
Value	Select **True**



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

6. Click **Save**.

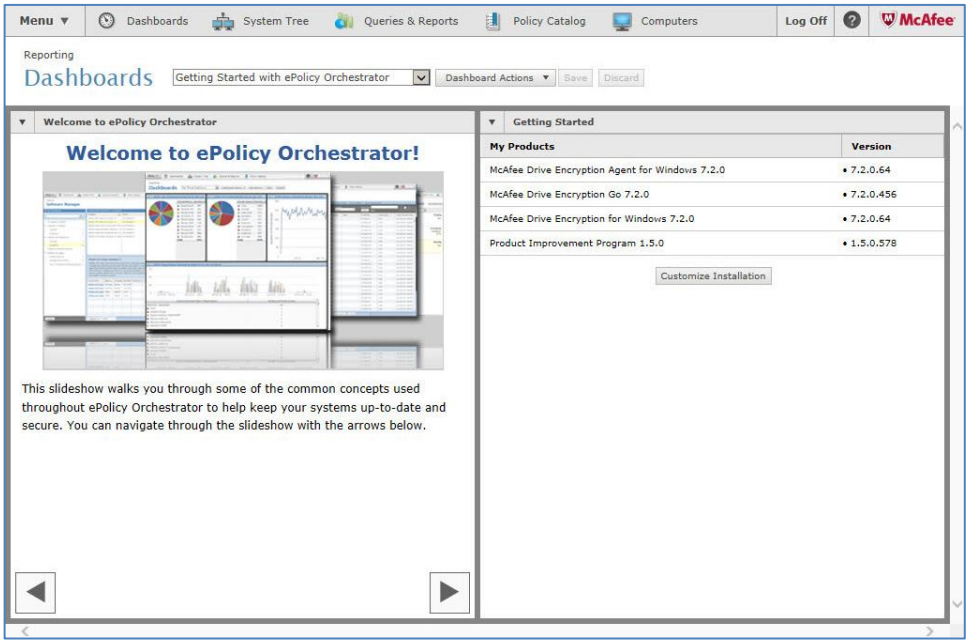
Configuring a Policy Assignment Rule

In this section we created a policy assignment rule based on username. Administrator can decide the type of policy assignment rule he wants to create.

1. Open the **ePolicy Orchestrator** Login page.

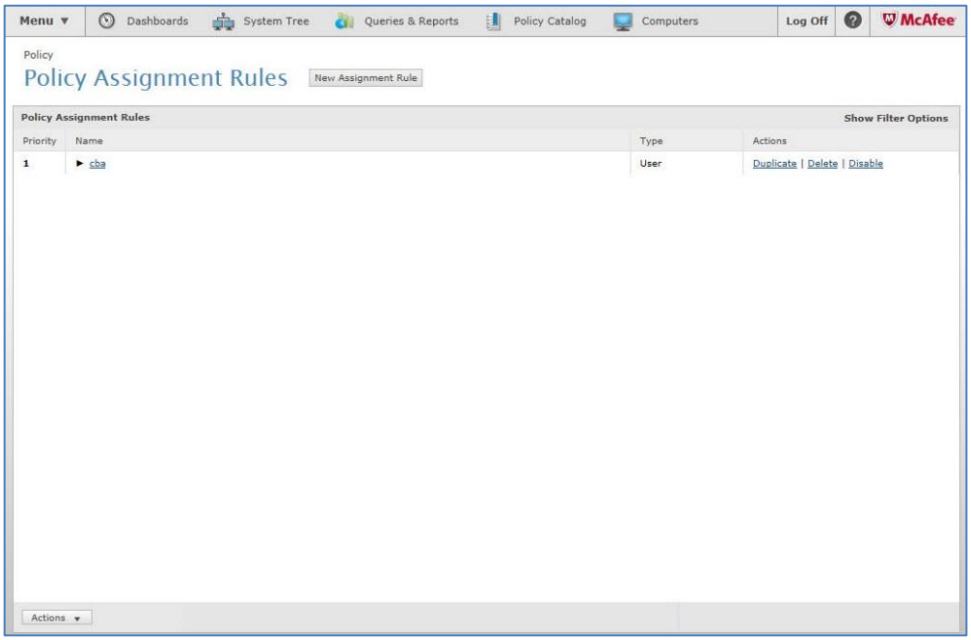
(The screen image above is from McAfee©. Trademarks are the property of their respective owners.)

2. Login to the admin console.



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

3. Select **Menu > Policy > Policy Assignment Rules.**



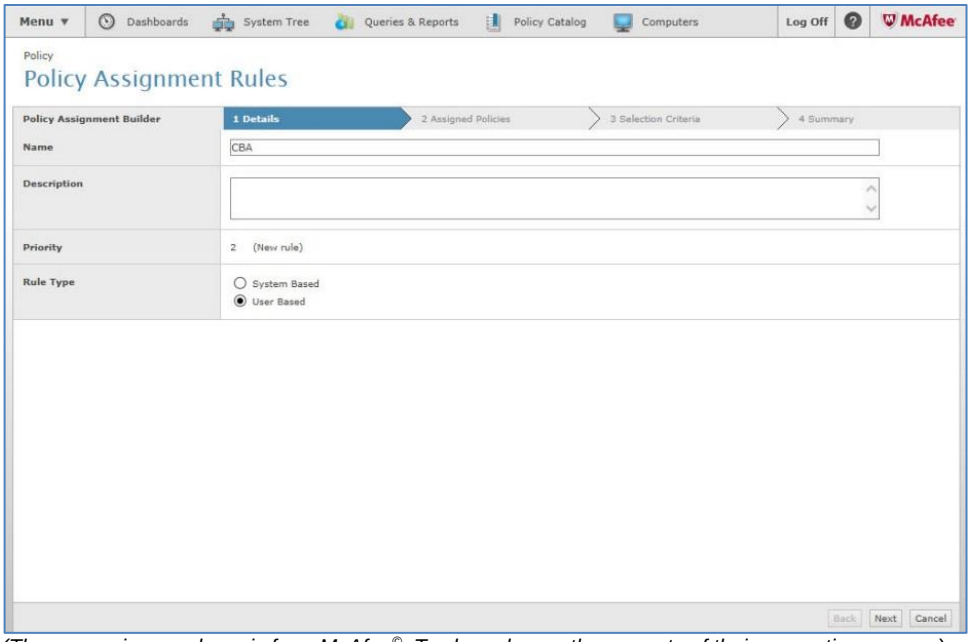
(The screen image above is from McAfee©. Trademarks are the property of their respective owners.)

4. Click on **New Assignment Rule**.

   The **New Assignment Rule** window is open.

5. In the **Details** tab, configure the following:

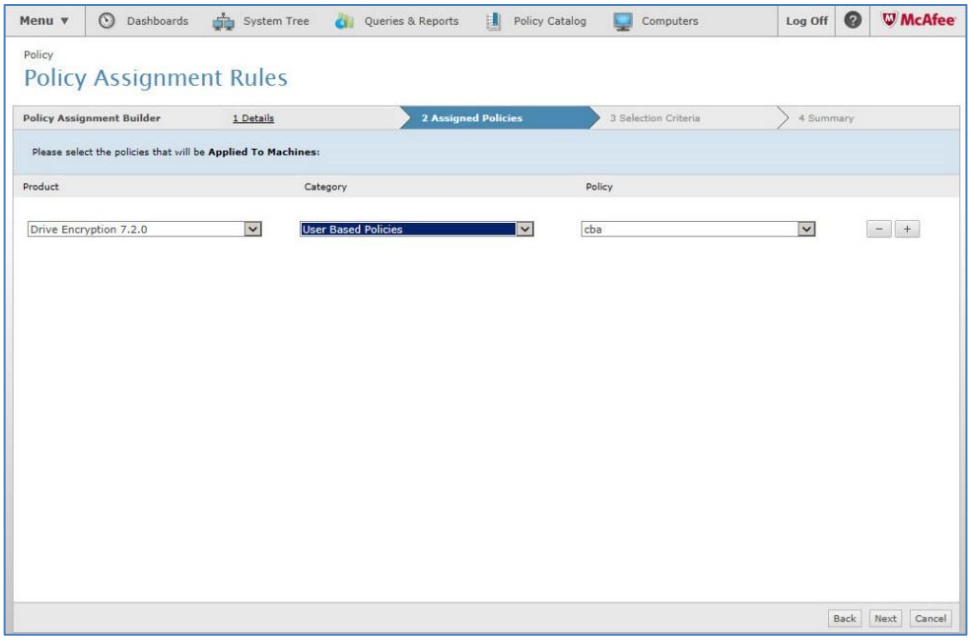
Field	Description
Name	Enter a name for the policy.
Rule Type	Select **User Based.**



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

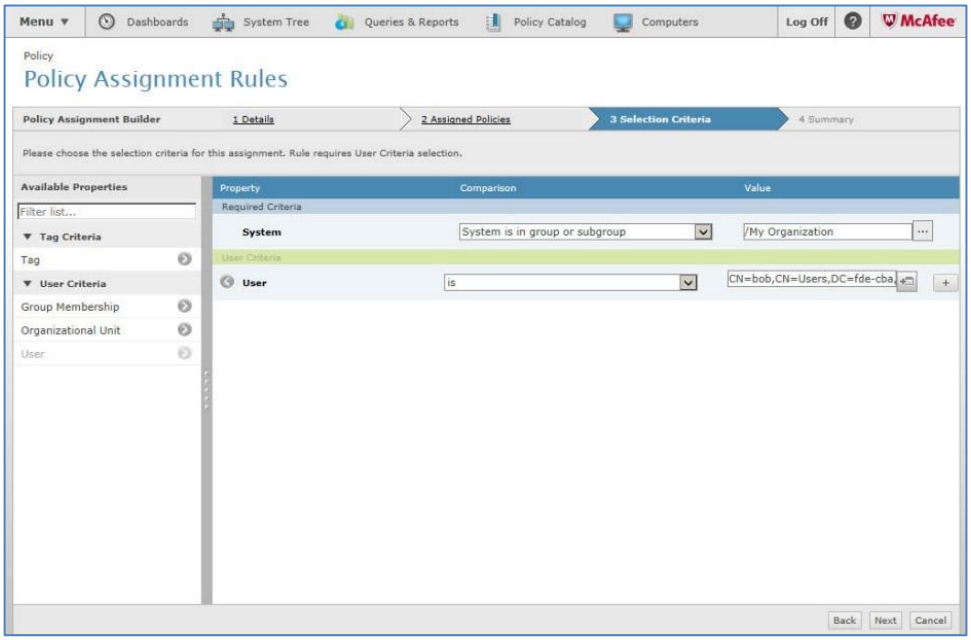
6. Click **Next**
7. In the **Assigned Policies** tab, click **Add Policy** and configure the following:

Field	Description
Product	Select the Drive Encryption product.
Category	Select **User Based Policies.**
Policy	Select the user-based policy you created previously.



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

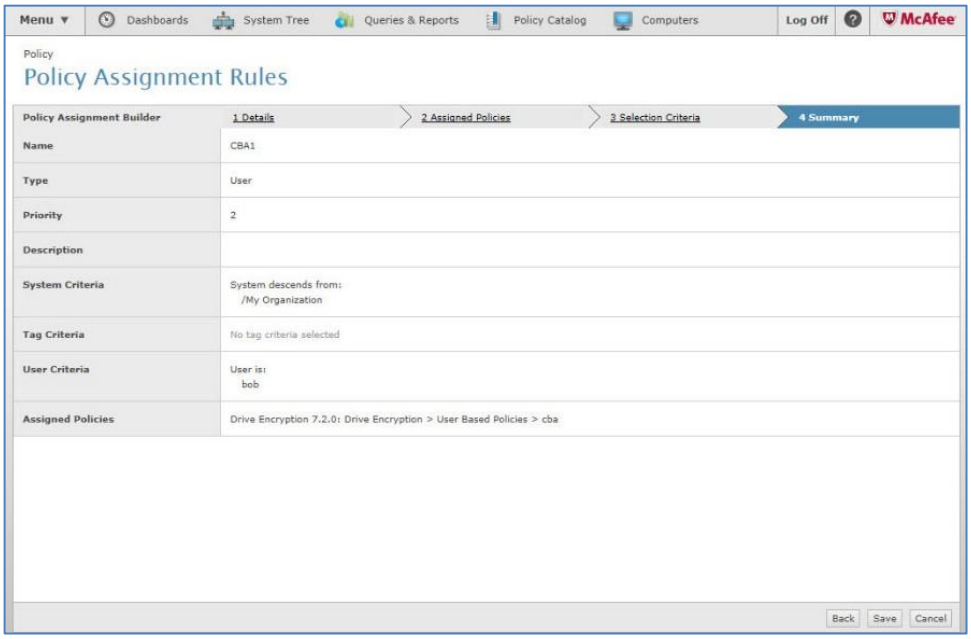
8. Click **Next.**
9. In the **Selection Criteria** tab select the system you are working on.
10. Click **Users** in the left pane and in the main pane select the users to which the policy needs to be assigned.



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

11. Click **Next**

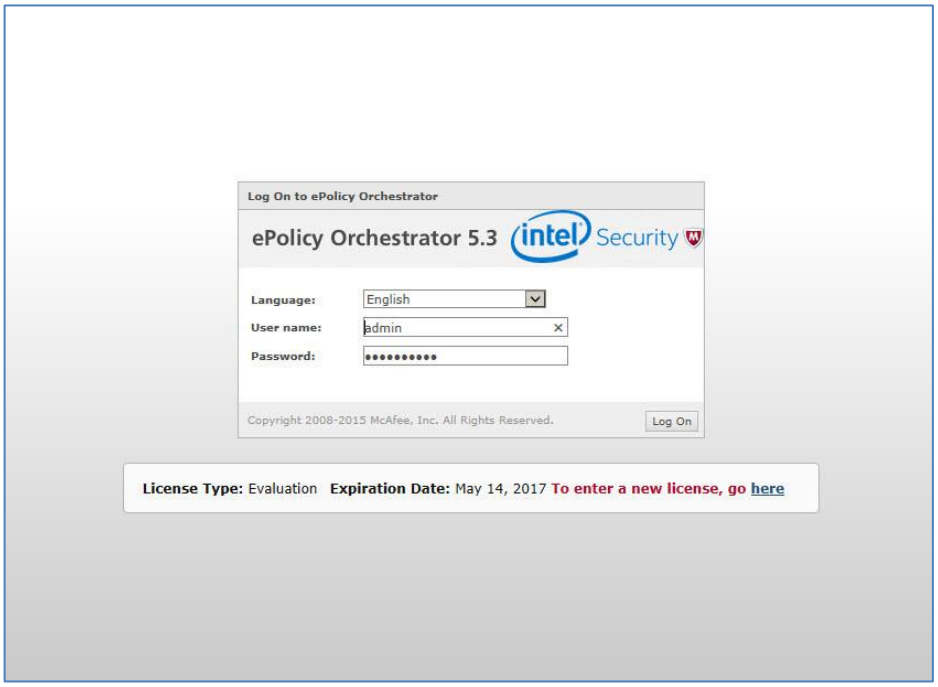
12. In the **Summary** tab, click **Save**



Assigning the Policy to a System

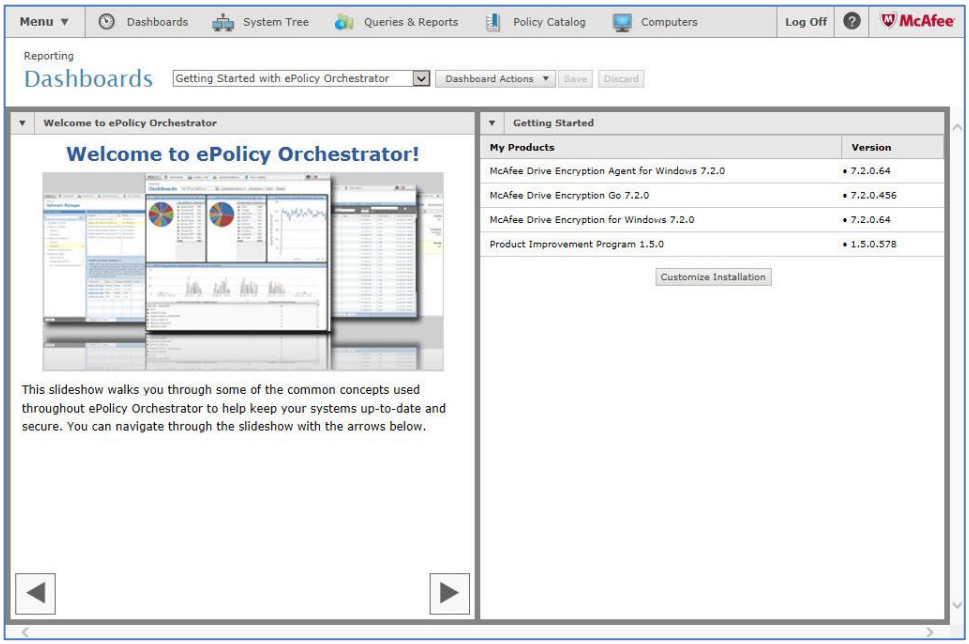
Now we need to assign the policy we created to the machine/machines that are already managed by the McAfee agent and that the McAfee Disk Encryption product is installed on.

1. Open the **ePolicy Orchestrator** Login page.



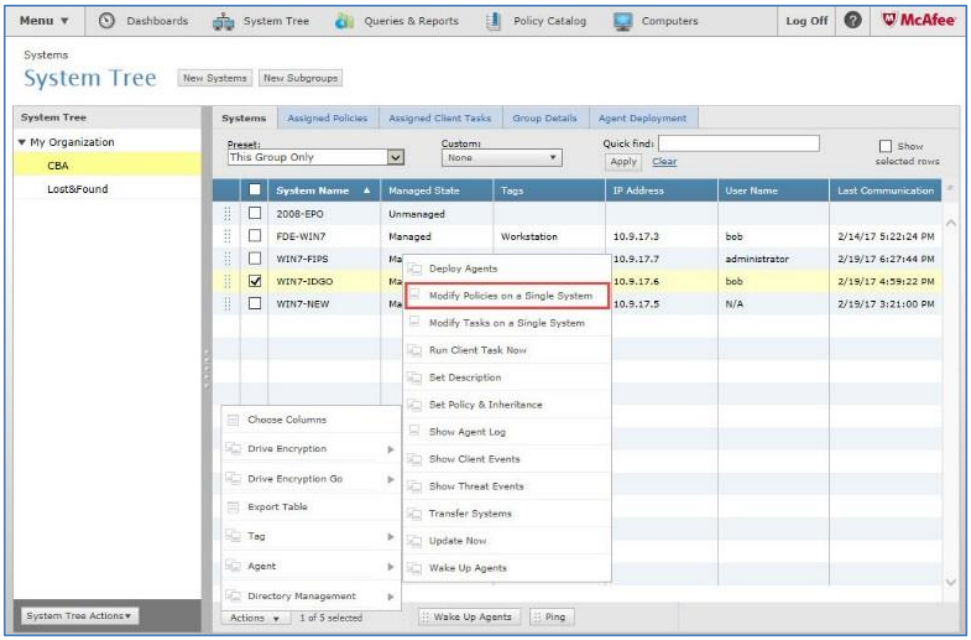
(The screen image above is from McAfee©. Trademarks are the property of their respective owners.)

2. Login to the admin console.



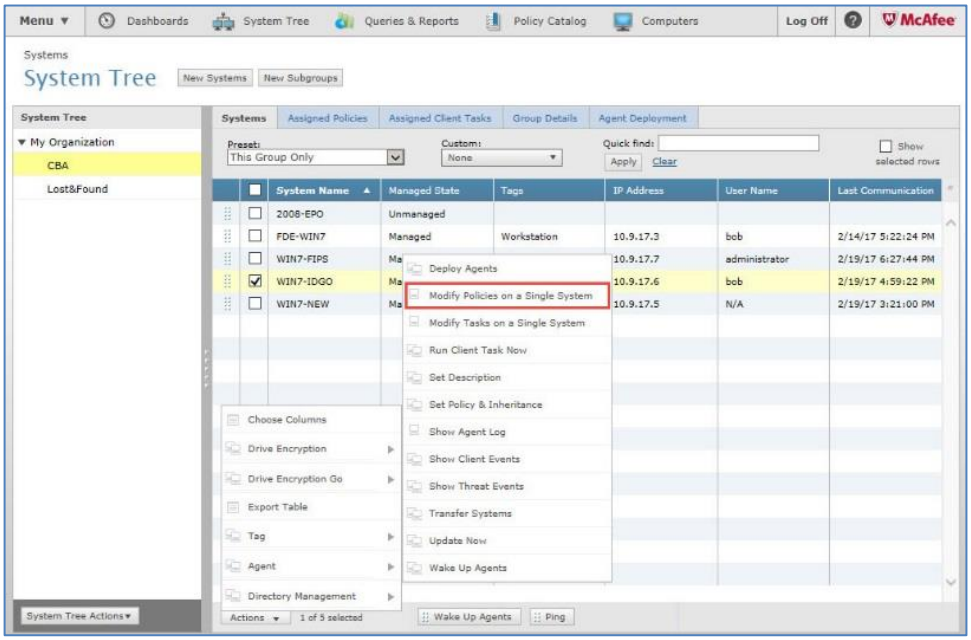
(The screen image above is from McAfee©. Trademarks are the property of their respective owners.)

3. Select **Menu > System > System Tree**.



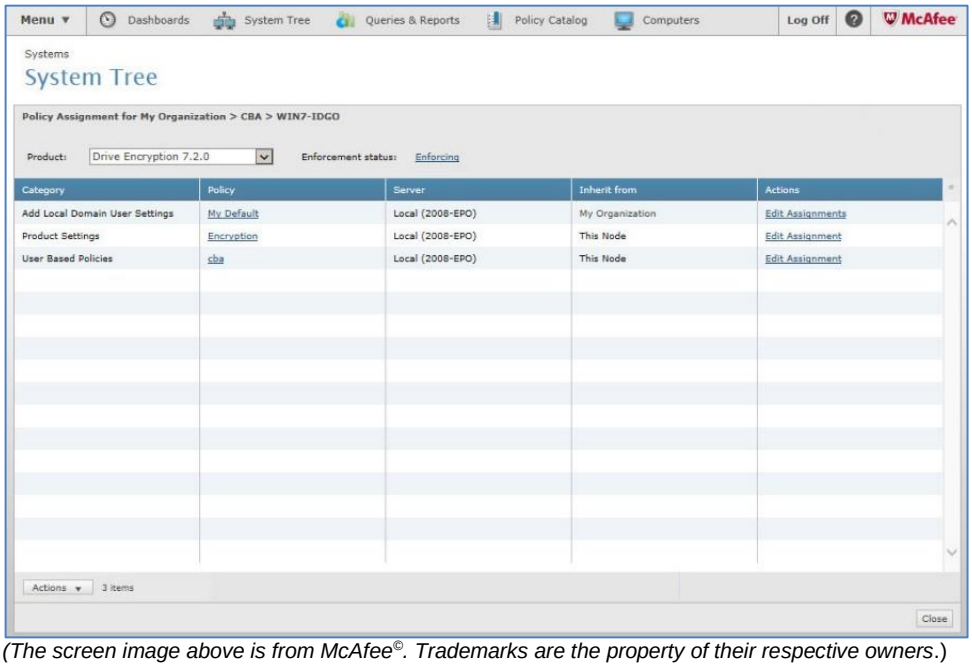
(The screen image above is from McAfee©. Trademarks are the property of their respective owners.)

4. Select the system/s upon which the CBA needs to be enforced and select **Actions > Agent** > **Modify Policies on a Single System.**



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

5. Under **Product** select the **Drive Encryption** product.



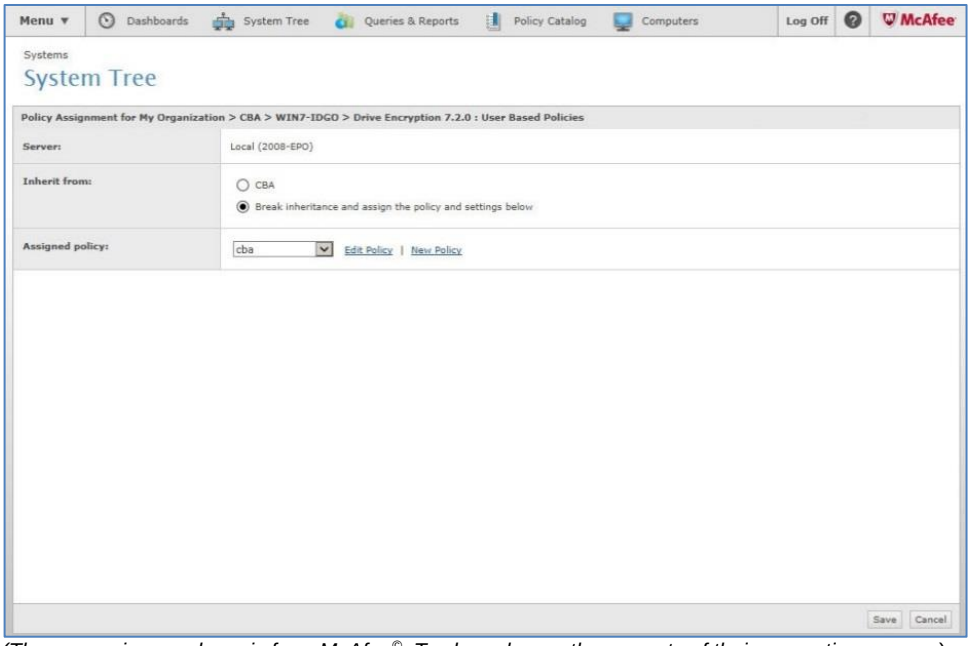
(The screen image above is from McAfee©. Trademarks are the property of their respective owners.)

6. Click the User Based Policy (cba in this example) **Edit Assignment** link.

   The edit assignment window opens.

7. Configure the following:

Field	Description
Inherit From	Select **Break inheritance and assign the policy and setting below**.
Assigned policy	Select the CBA policy you created**.**



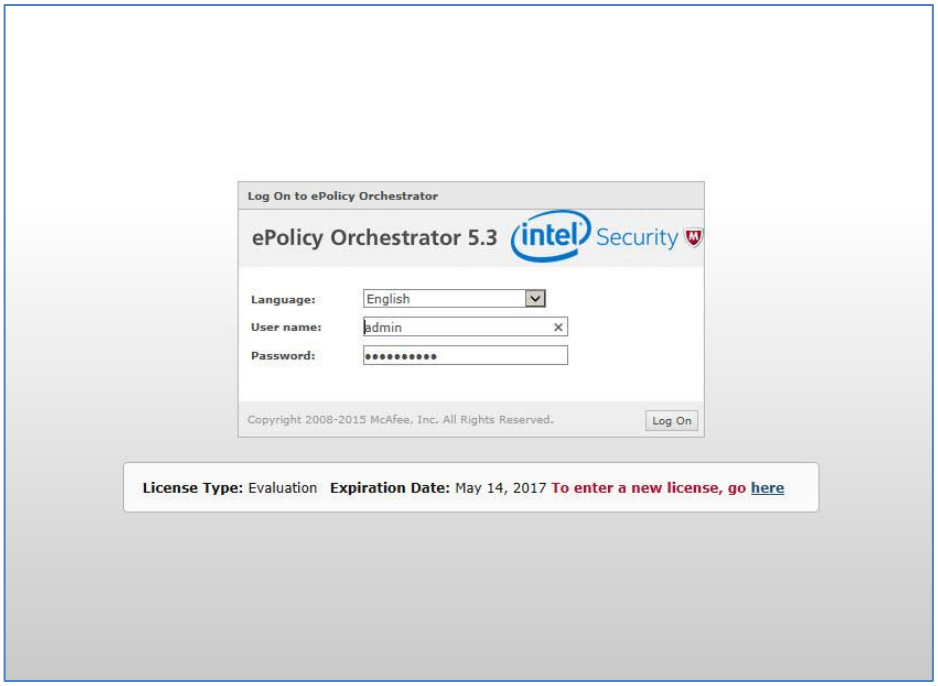
(The screen image above is from McAfee©. Trademarks are the property of their respective owners.)

8. Click **Save**.

Configuring User-Based Policy Enforcement

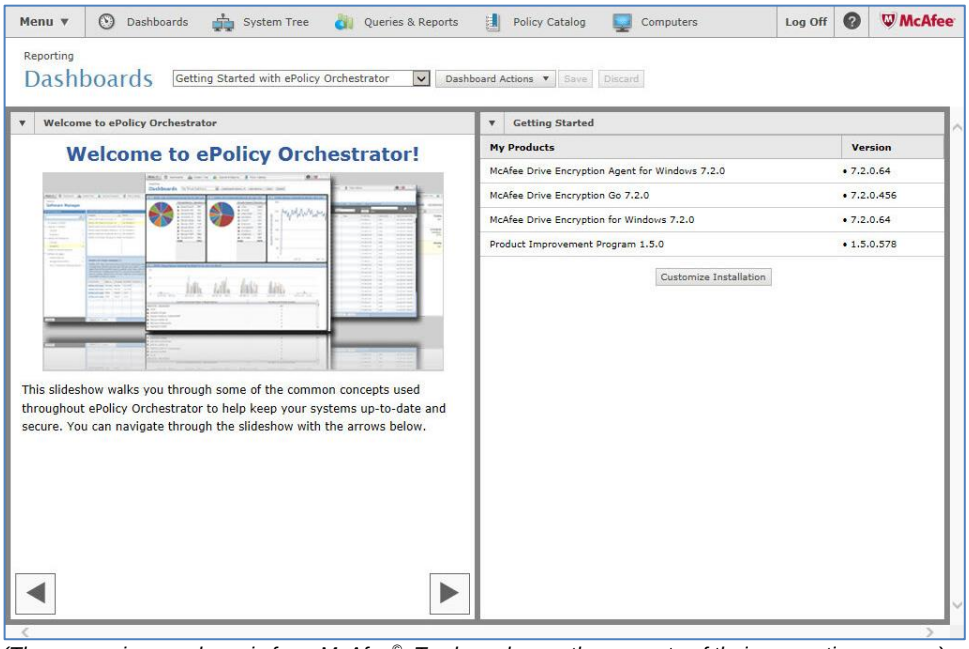
In order for the user to use the CBA policy you created it needs to be configured in the ePolicy Orchestrator.

1. Open the **ePolicy Orchestrator** Login page.



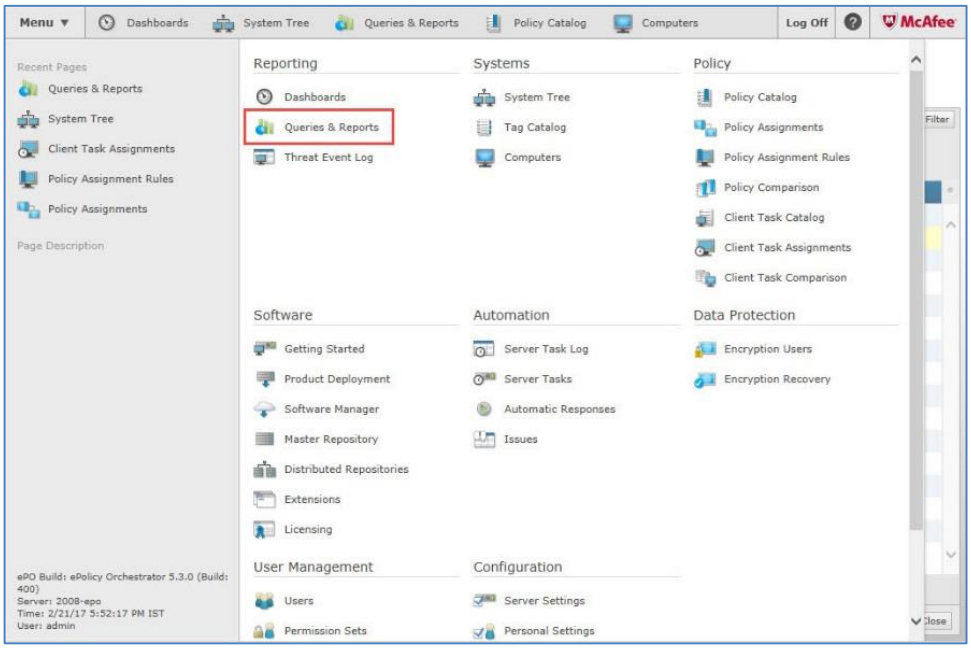
(The screen image above is from McAfee©. Trademarks are the property of their respective owners.)

2. Login to the admin console.



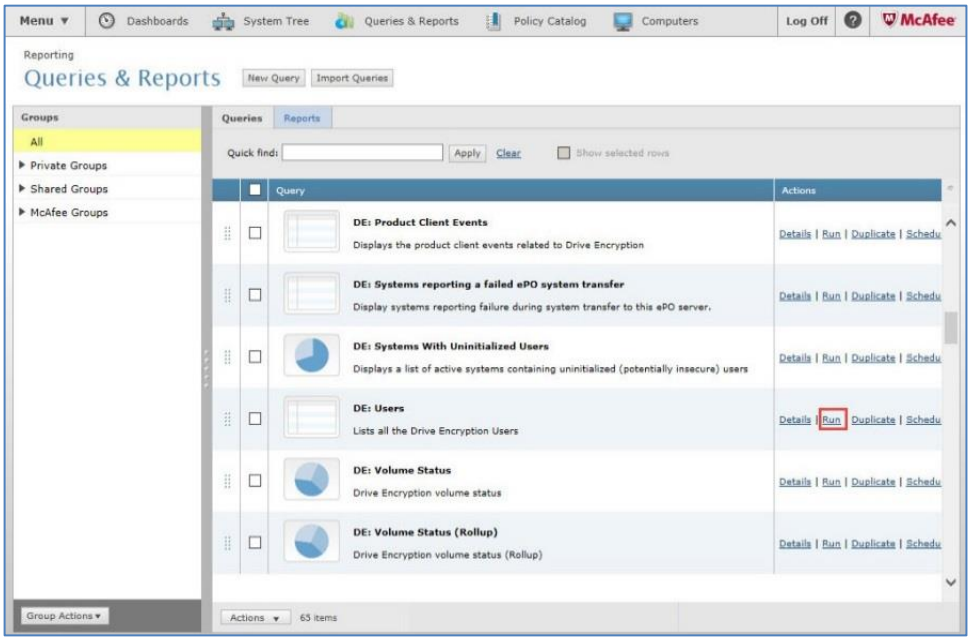
(The screen image above is from McAfee©. Trademarks are the property of their respective owners.)

3. Select **Menu >Reporting > Queries & Reports.**



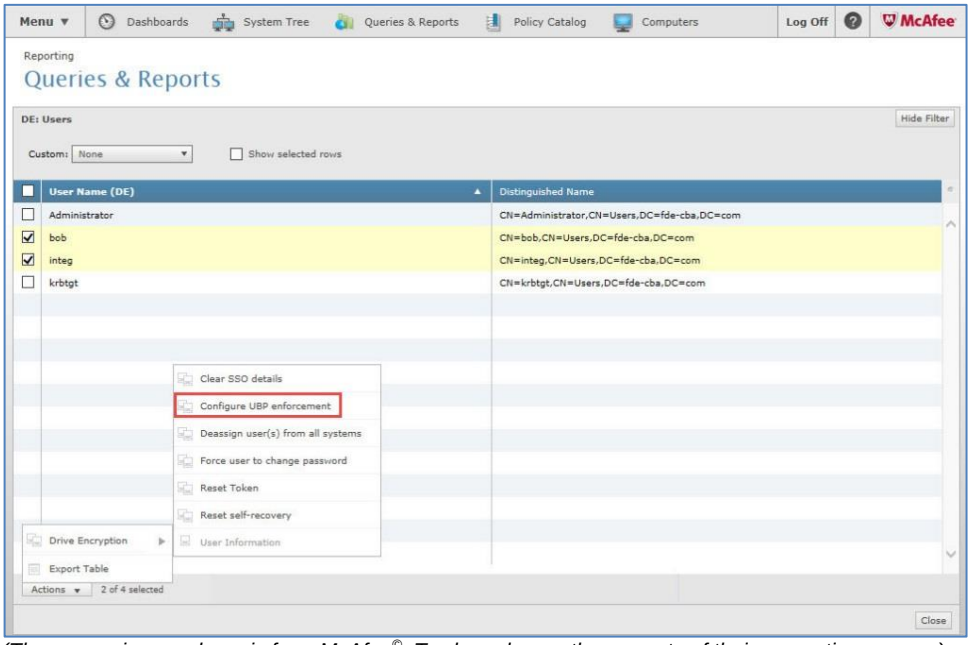
(The screen image above is from McAfee©. Trademarks are the property of their respective owners.)

4. Under **Query** select **DE: Users** and click **Run.**



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

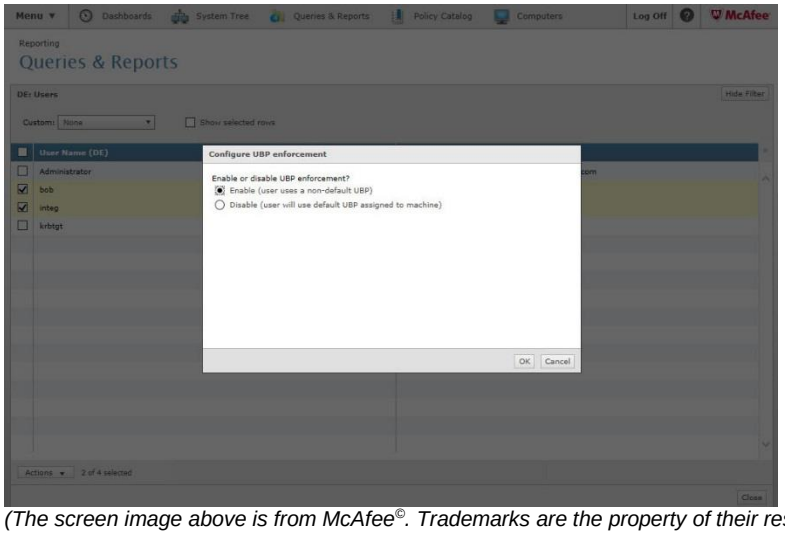
5. Select the users to be configured and select **Actions > Drive Encryption > Configure UBP enforcement.**



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

The **Configure UBP enforc**ement window opens.

6. Select **Enable (user users a non-default UBP)** and click **OK**.



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

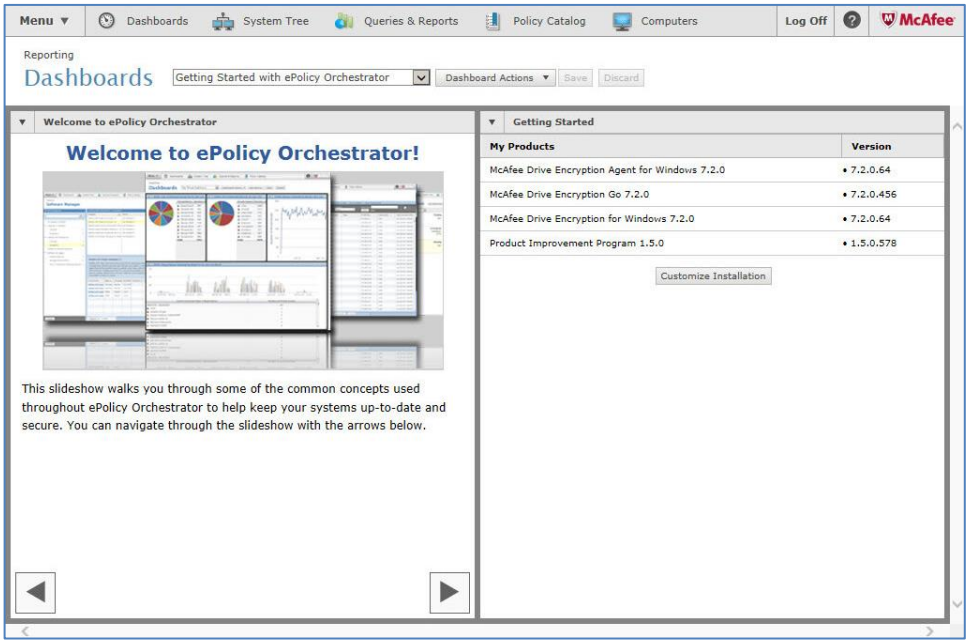
Update the Client Machine

In order for the changes to take affect you need to update the client machine with the new policies.

1. Open the ePolicy Orchestrator Login page.

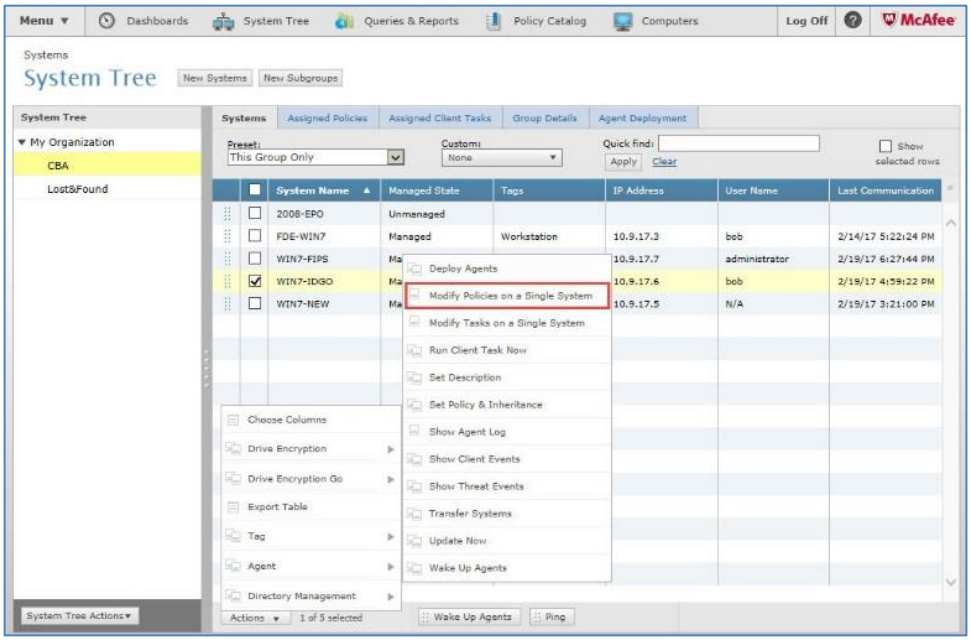
(The screen image above is from McAfee©. Trademarks are the property of their respective owners.)

2. Login to the admin console.



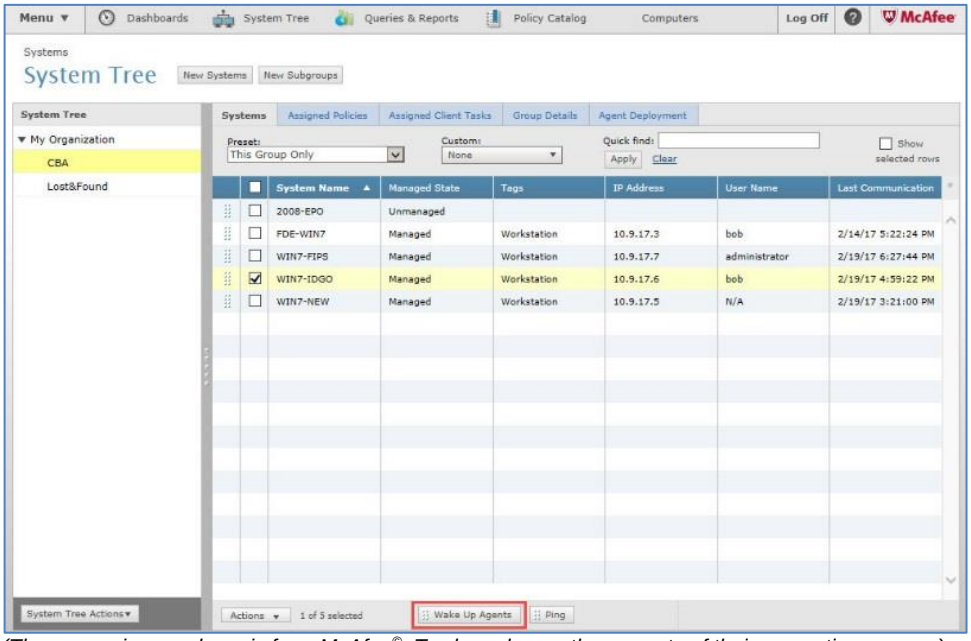
(The screen image above is from McAfee©. Trademarks are the property of their respective owners.)

3. Select **Menu > System > System Tree**.



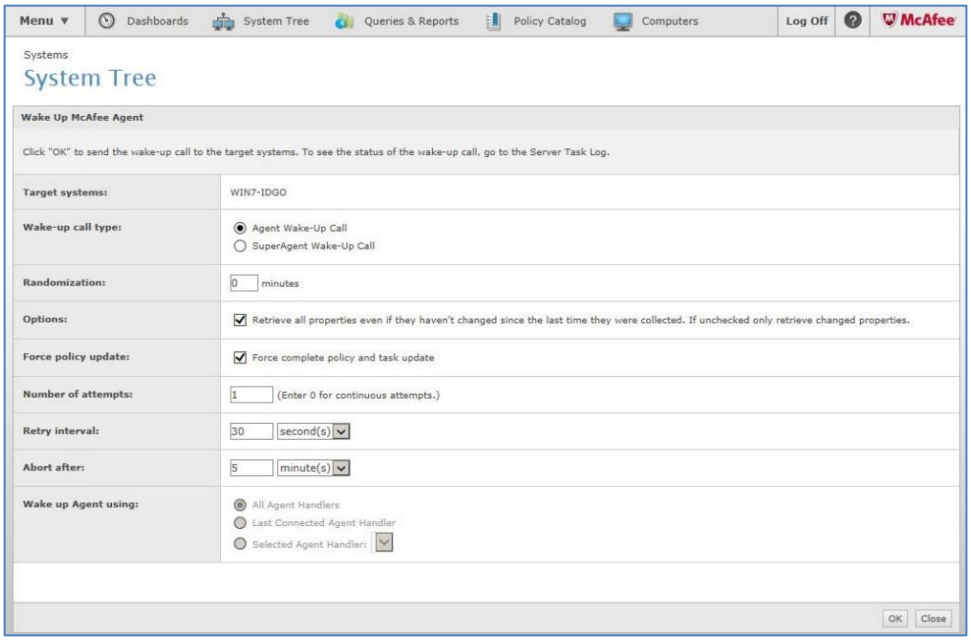
(The screen image above is from McAfee©. Trademarks are the property of their respective owners.)

4. Select the system/s on which the CBA needs to be enforced on and click **Wake Up Agents.**



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

5. Select **Force complete policy and task update**.



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

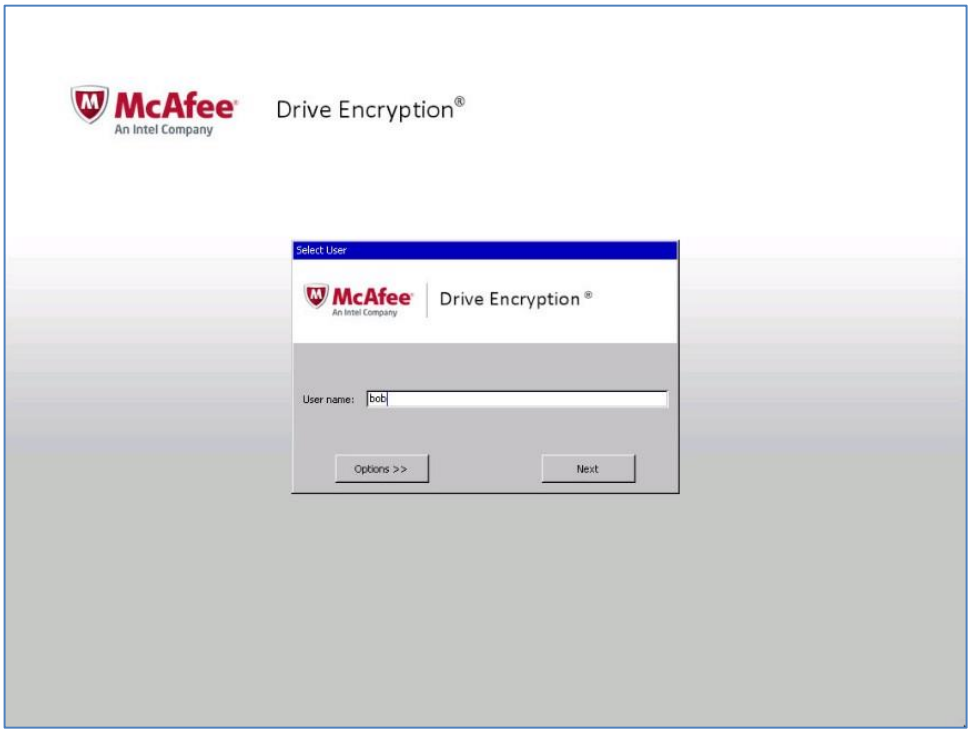
6. Click **OK.**

   The client machine is updated.

Running the Solution

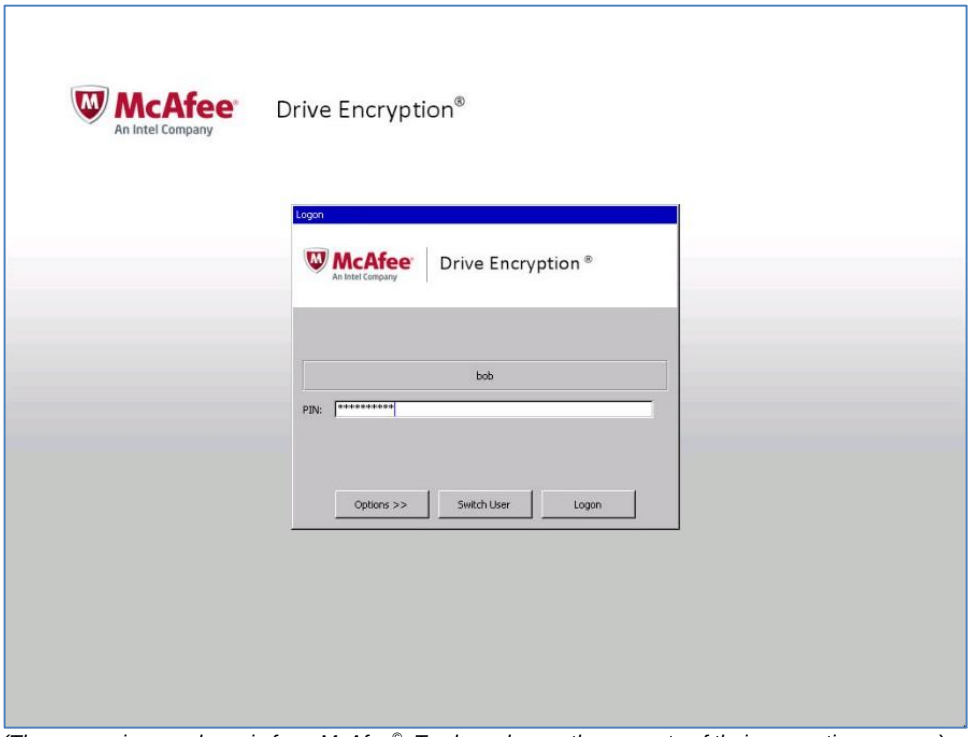
This section demonstrates the pre-boot authentication process.

1. Start the client machine and insert the Gemalto token/smart card.
2. In the first screen enter the username and click **Next**.



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

3. Enter the token/smart card PIN and click **Logon.**



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

After a successful authentication the machine boots.

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 Gemalto Customer Support. Gemalto 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 Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information
Customer Support Portal	https://supportportal.gemalto.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.
Technical Support contact email	technical.support@gemalto.com