Symantec™

Symantec Endpoint Encryption Full Disk

Windows User Guide

Version 8.2.0

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043
http://www.symantec.com

Contents

Figures

1. Introduction

Overview

Symantec Endpoint Encryption Full Disk ensures that only authorized users can access data stored on hard disks. This safeguards enterprises from the accidental loss or theft of a laptop or PC and eliminates the legal need for public disclosure. As a key component of Symantec Endpoint Encryption, Full Disk offers seamless deployment and operation across diverse IT infrastructures and environments.

This Guide includes chapters on registering for an account; using the User Client Console; authenticating in pre-Windows with a password or a token; and obtaining logon assistance for forgotten passwords, PINs, or tokens.

This chapter introduces basic concepts such as registration, authentication, encryption, the User Client Console, administrator roles, and describes best practices for securing your computer.

The sections are as follows:

- “Basic Concepts” on page 1
- “Best Practices” on page 2

Basic Concepts

Registration

All users must have a Symantec Endpoint Encryption account to complete pre-boot authentication and access the User Client Console. Accounts are created through the registration process.

Registration is a highly configurable process:

- Your Policy Administrator may or may not have required you to enter a registration password. The registration password, if required, will be necessary to begin the registration process.
- You may be required to step through a Registration wizard or your Policy Administrator may have configured registration to take place automatically, without any intervention.

Encryption

Full Disk also protects the data stored on your hard disk by encrypting it. Encryption is the process by which an algorithm renders data unreadable. Only those in possession of the “key” can decrypt the data, thereby rendering it intelligible again. Most likely the encryption was configured to happen immediately following the installation of Full Disk. Encryption is transparent to you. You can continue to work normally during and after the encryption of your hard disk(s). All partitions should be encrypted, especially the Windows system partition.

Authentication

Full Disk protects the data stored on your hard disk by requiring you to authenticate before it allows Windows to load. When you provide your credentials to Full Disk it derives the “key” necessary to render the data on your hard disk intelligible again. Authentication could have been configured to occur in one of three ways:

- *Single Sign-On (SSO) enabled*—You will be prompted to authenticate once, each time your computer is restarted.
- *Single Sign-On not enabled*—You must log on in pre-Windows to Full Disk and then separately to Windows.
- *Automatic authentication enabled*—You will not be prompted to provide credentials to Full Disk; the process will be transparent to you.

The User Client Console

The User Client Console is available once Windows has loaded and allows you to:

- View the encryption status of your hard disk partitions.
- View the other registered users on your computer.
- View the last time your computer checked in with the Symantec Endpoint Encryption Management Server, if at all.
- View product version information.
- Encrypt hard disk partitions that are decrypted, if any.

In addition, you might be able to:

- Add or change the password you use to authenticate to Symantec Endpoint Encryption.
- Add or change the token you use to authenticate to Symantec Endpoint Encryption.
- Add or change your Authenti-Check questions and answers.
- Force your computer to check in with the Symantec Endpoint Encryption Management Server.
- View, set, or reset the Novell account information associated with your Windows account information.
- Decrypt hard disk partitions.

Policy Administrators

A Policy Administrator performs centralized administration activities, such as defining installation settings and policies, and issuing encryption and decryption commands. The Policy Administrator runs the help-desk side of the One-Time Password Program to assist you in unlocking your locked computer or recovering from a forgotten password, token, or PIN.

Client Administrators

A Client Administrator provides local support to users and can help you if you get locked out of your computer, forget your password, token, or PIN; or if your computer fails to boot.

Best Practices

Password/PIN Secrecy

You are responsible for the security of your password or PIN. Change your password or request a new PIN if you feel that it may have been compromised. Some situations to be mindful of are:

- You wrote your password or PIN on a piece of paper but now you can’t find that paper.
- Someone looked over your shoulder and watched you type your password or PIN.

Authenti-Check Questions and Answers

If you have Authenti-Check available, you will be prompted to define up to three question-answer pairs. If you forget your Symantec Endpoint Encryption password, you can authenticate to Full Disk by correctly answering the questions.

Most likely, you will define the question-answer pairs during registration. If your administrator enables this feature following registration, you will be prompted during your Windows session to define the question-answer pairs using the User Client Console. Until you define the question-answer pairs, you will not have this recovery method available.

The Authenti-Check questions and answers are just as important as your password or PIN. Do not let others watch you enter them. The question-answer pairs will be displayed in plain text onscreen as you enter them. Therefore, be especially mindful of anyone looking over your shoulder.

Computer Shutdown

It is best not to leave your computer unattended, particularly in an insecure location, such as a cafe. If you must step away, you should press the Windows logo key+L to invoke the Windows logon. To achieve Full Disk protection, you must power the machine down.

Trusted Software

Be familiar with the software that is authorized to run on your computer. Be careful if you download software from the Internet. This software could contain spyware, viruses, malware, Trojan horses, or worms. Also use caution when opening email attachments.

Backups

If your organization does not perform automated backups, you should do so yourself on a regular basis. This will allow you to recover from theft or hard disk failure. Store your backups in a physically secure location, such as a locked cabinet.

2. Registration & Re-Registration

Overview

One of the first signs that Full Disk has been installed may be a prompt for registration. If you are prompted to register, you are encouraged to do so as soon as possible, even if it is not yet mandatory. The registration of the first user greatly improves the ability of Full Disk to protect your computer.

You also may be prompted to re-register. This can occur if your organization is switching authentication methods.

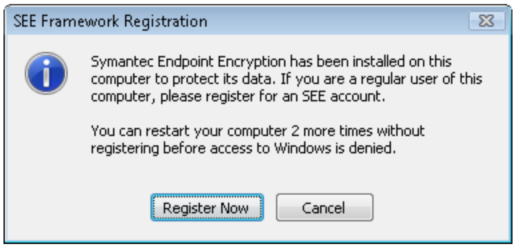
Registration Prompts

Basics

After Full Disk is installed and your computer reboots, if you haven’t registered already, you may be prompted to do so.

Grace Restarts Available

Grace restarts are the number of times you can reboot without having to register. The following figure shows a sample of a message you may receive if your Policy Administrator has given you grace restarts.



Symantec Endpoint Encryption has been installed on this computer to protect its data. If you are a regular user of this computer, please register for an SEE account.

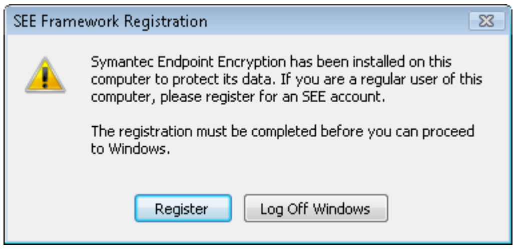
You can restart your computer 2 more times without registering before access to Windows is denied.

Figure 2.1—Registration Prompt, Grace Restarts Available

The prompt informs you that you can restart a set number of times without having to register. While you can click **Cancel** and continue working normally, it’s best to click **Register Now** and begin the registration process (see “Registration Wizard” on page 6).

Registration Mandate

Once your grace restarts expire, or if your Policy Administrator did not give you any grace restarts, you will be forced to register. The following figure shows a sample of a message you will receive if your Policy Administrator has not given you grace restarts.



Symantec Endpoint Encryption has been installed on this computer to protect its data. If you are a regular user of this computer, please register for an SEE account.

The registration must be completed before you can proceed to Windows.

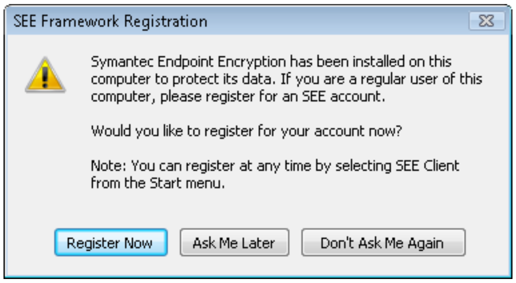
Figure 2.2—Registration Prompt, Mandate

Registration takes only a few moments. Click **Register** to begin the registration process (see “Registration Wizard” on page 6).

If you can’t complete registration now, click **Log Off Windows**. The next time you try to log on to Windows, you will receive the same registration mandate. You will be unable to use Windows until you register.

Multiple Users

If at least one user has already registered to Symantec Endpoint Encryption, you may be prompted to register on an optional basis.



SEE Framework Registration

Symantec Endpoint Encryption has been installed on this computer to protect its data. If you are a regular user of this computer, please register for an SEE account.

Would you like to register for your account now?

Note: You can register at any time by selecting SEE Client from the Start menu.

Figure 2.3—Registration Prompt, Multiple Users

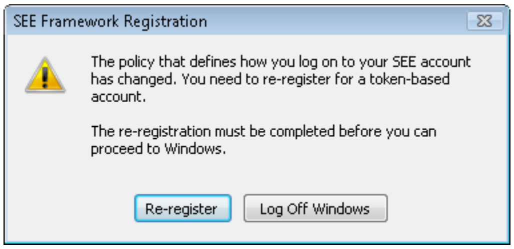
Click **Register Now** to begin the registration process (see “Registration Wizard” on page 6).

If you click **Ask Me Later** or **Don’t Ask me Again**, you will be unable to authenticate in pre-Windows. This could be appropriate if you need to use the computer only this one time or will never need to boot it up from a powered-off state.

Re-Registration

Your Policy Administrator may change your method of authentication, either using a policy or an upgrade. Should this occur, you will be required to re-register.

The following figure shows the sample prompt for re-registering for a token authentication method.



SEE Framework Registration

The policy that defines how you log on to your SEE account has changed. You need to re-register for a token-based account.

The re-registration must be completed before you can proceed to Windows.

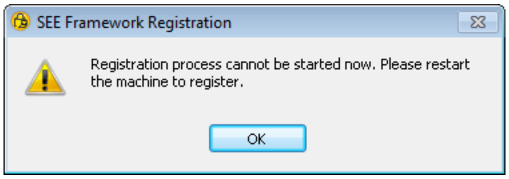
Figure 2.4—Re-Registration Mandate

Click **Re-register** to launch the Registration wizard. If you need to re-register for a password-based account, follow the instructions under “Password Registration” on page 9. If you need to re-register for a token-based account and you have been issued your token, follow the instructions under “Token Registration” on page 12.

If you can’t complete re-registration, click **Log Off Windows**. This could occur if you receive the prompt before you receive your token. The next time you boot up, you can authenticate in pre-Windows with your existing Symantec Endpoint Encryption account, but when you try to log on to Windows, you will receive the same re-registration mandate.

Reboot to Register

On computers without Opal-compliant drives, the 65th, 129th, 193rd, 257th, 321st, 385th, 449th, 513th, 577th, 641st, 705th, 769th, 833rd, 897th, and 961st user cannot register right away. These users receive the following message upon logging onto Windows or attempting to launch the User Client Console.



Registration process cannot be started now. Please restart the machine to register.

Figure 2.5—Registration Process Cannot be Started Now

Only registered users and Client Administrators can complete Pre-Windows authentication. To register after receiving the “Registration process cannot be started now” message:

1. Find someone with valid Symantec Endpoint Encryption credentials, i.e., a registered user or a Client Administrator.
2. Have the registered user or Client Administrator shut down and log on to Pre-Windows.
3. Log on to Windows using your own credentials.
4. Click **Register Now** to initiate the registration process.

Registration Wizard

Basics

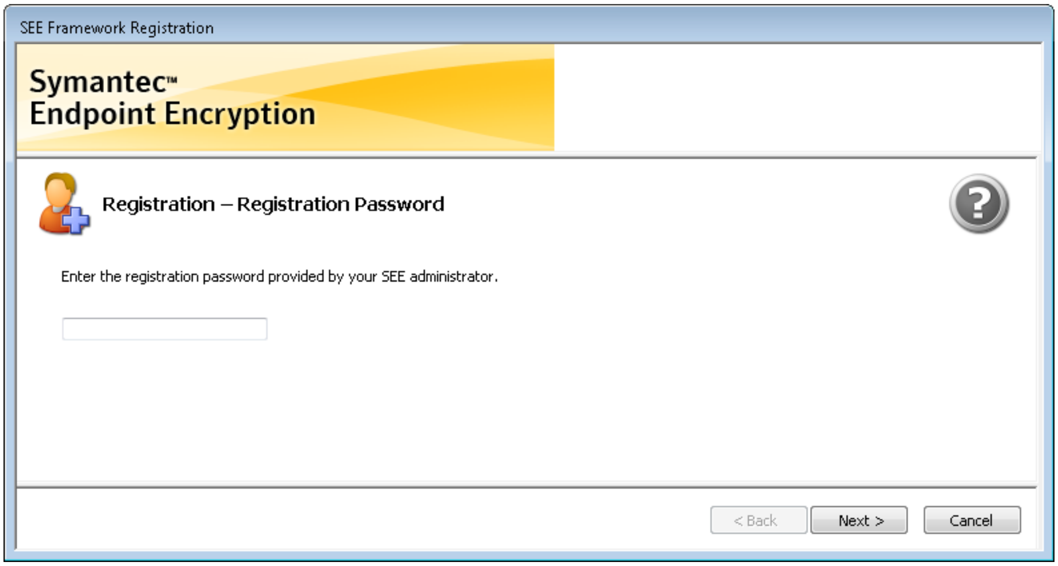
The Registration wizard guides you through the registration process. This wizard is the same for both registration and re-registration. The steps in this process will vary according to how your computer has been configured.

If you click **Cancel** in the Registration Wizard, your Symantec Endpoint Encryption account will not be created. You will be prompted to confirm that you really want to cancel.

To display Quick Help, click the help icon ?. The Quick Help pane appears. To close the Quick Help pane, click the help icon again.

Registration Password

You may need a password to begin the registration process. If you don’t see the Registration Password panel, you don’t need to enter a registration password. Skip to the next section (“Preferred Authentication Method” on page 7).


SEE Framework Registration
Symantec™
Endpoint Encryption
Registration – Registration Password

Enter the registration password provided by your SEE administrator.

Figure 2.6—Registration, Registration Password

A registration password is a way for your administrator to limit the number of users allowed to register on this computer. The registration password is not your Symantec Endpoint Encryption password; the registration password admits you to the registration process.

You should have received this password ahead of time. If you do not have the password, call your help desk or click **Cancel**.

Otherwise, type the password and click **Next**.

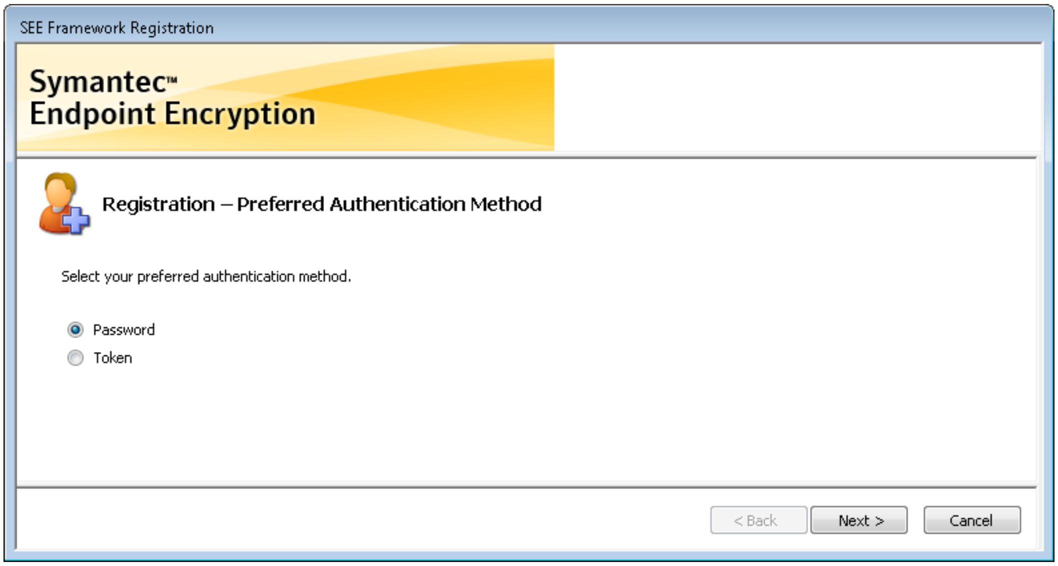
If the password is accepted, the next panel in the registration process appears.

If the password is not accepted, a message appears and you will need to correct it before you can proceed. Re-enter the password then click **Next** to resubmit it, or click **Cancel**. The **Back** button is not available.

Preferred Authentication Method

If your administrator has chosen to allow you to authenticate with either a password or a token and Single Sign-On is not enabled, the Preferred Authentication Method panel will be displayed. If the Preferred Authentication Method panel is not displayed, refer to the section that corresponds to your authentication method:

- If you authenticate with a password, skip to “Password Registration” on page 9.
- If you authenticate with a token, skip to “Token Registration” on page 12.
- If you don’t authenticate (automatic authentication), skip to “Completion” on page 15.



Registration – Preferred Authentication Method

Select your preferred authentication method.

● Password
○ Token

Figure 2.7—Registration, Preferred Authentication Method

Select the method of authentication that you prefer and select **Next**. If you select **Password**, continue to the next section. If you select **Token**, skip to “Token Registration” on page 12.

While the Registration Wizard will only escort you through your preferred authentication method, you can add a second method using the User Client Console at any time following registration.

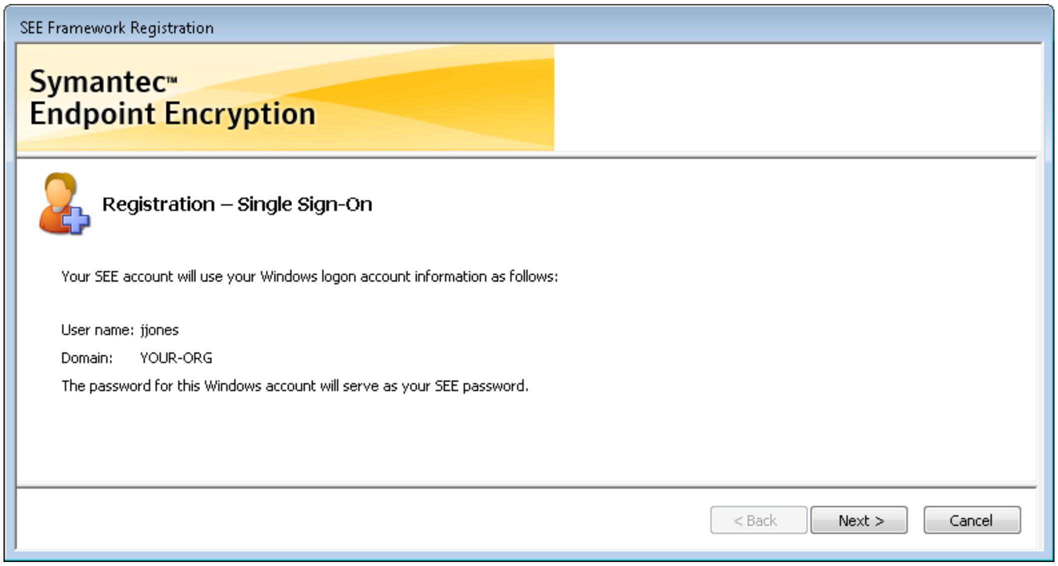
Password Registration

Basics

The password registration process will vary according to whether or not you have Single Sign-On enabled.

Single Sign-On Enabled: Windows

If Single Sign-On is enabled, you will see a Single Sign-On panel. If you don't see this panel, skip to "Single Sign-On Not Enabled" on page 11.



Your SEE account will use your Windows logon account information as follows:

User name: jjones
Domain: YOUR-ORG
The password for this Windows account will serve as your SEE password.

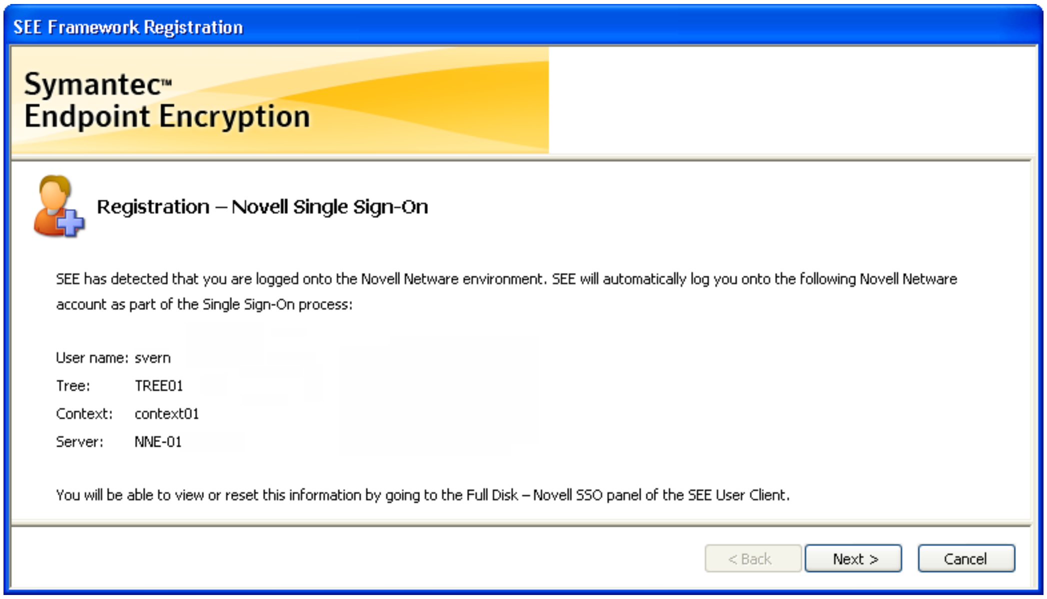
Figure 2.8—Password Registration, SSO Enabled, Windows Account Information

The credentials associated with your Windows account will be used for your Symantec Endpoint Encryption account.

Click **Next** to continue. If you have Novell installed, continue reading. If not, skip to "Authenti-Check" on page 14.

Single Sign-On Enabled: Novell

If your organization uses Novell and you are logged on to Novell, you should see the Novell Single Sign-On panel. If not, skip to “Authenti-Check” on page 14.



Registration – Novell Single Sign-On

SEE has detected that you are logged onto the Novell Netware environment. SEE will automatically log you onto the following Novell Netware account as part of the Single Sign-On process:

User name: svern
Tree: TREE01
Context: context01
Server: NNE-01

You will be able to view or reset this information by going to the Full Disk – Novell SSO panel of the SEE User Client.

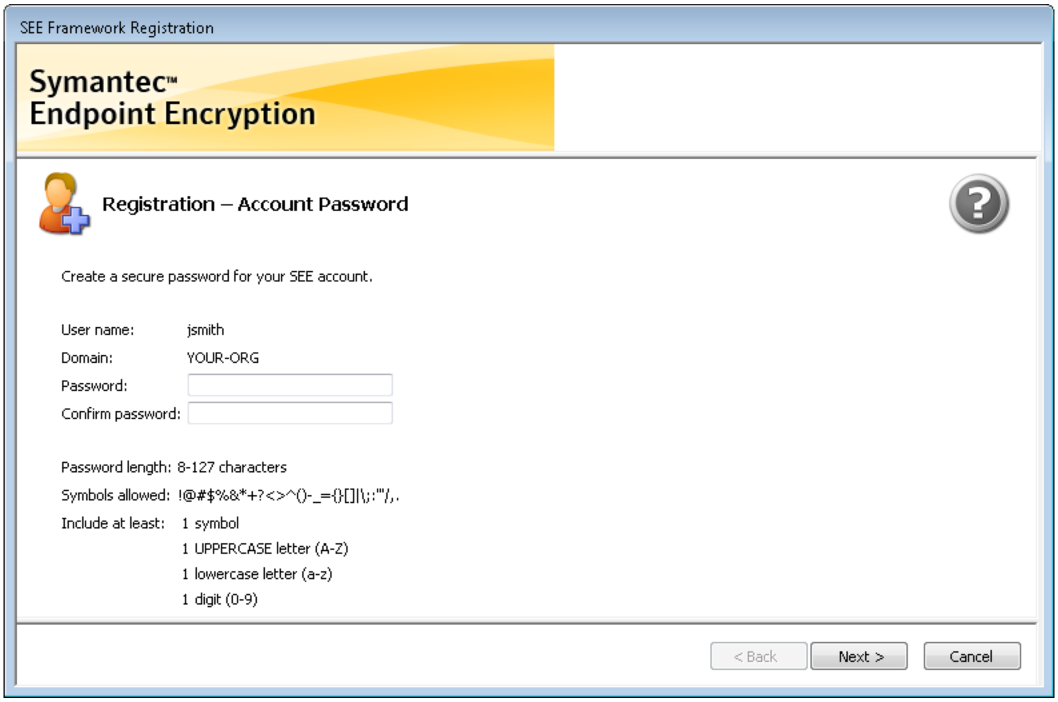
Figure 2.9—Password Registration, SSO Enabled, Novell Account Information

Full Disk will synchronize your Windows and Novell accounts with your Symantec Endpoint Encryption account so that you only have to log on once each time you turn on your computer.

Click **Next** to continue. Skip to “Authenti-Check” on page 14.

Single Sign-On Not Enabled

If Single Sign-On is not enabled, the Account Password panel will be displayed.



Registration – Account Password

Create a secure password for your SEE account.

User name: jsmith
Domain: YOUR-ORG
Password:
Confirm password:

Password length: 8-127 characters
Symbols allowed: !@#$%&*+?<>^()-_={}[]|\;:'"/,.
Include at least: 1 symbol
1 UPPERCASE letter (A-Z)
1 lowercase letter (a-z)
1 digit (0-9)

Figure 2.10—Password Registration, Account Password

The Account Password panel will display the account information of the user currently logged on to Windows.

Define a password that you can remember, so that you don't have to write it down. Longer passwords are more secure than short passwords. Include a variety of characters, including upper and lowercase letters mixed with numbers and special characters, if allowed. When you create a password, think of one that is hard to guess; for example, don't use a commonly known fact, such as your spouse's name, or a fact that can be easily researched, such as your mother's maiden name.

Follow the guidelines shown below the **Confirm password** field, if any. The password must be within the **Password length** specified. The **Symbols allowed** parameter identifies which of the symbols on your keyboard may be included in the password. The **Include at least** field identifies the number of required symbols, uppercase letters, lowercase letters, and/or digits that your password must contain, if any.

When creating your password, only enter characters that can be typed from the keyboard. Using alternate input methods—such as typing from the ALT+numeric keypad—may create characters that you will not be able to enter in the pre-Windows environment. If you have questions about keyboard use, please ask your Client Administrator.

Tab to or click on the **Confirm password** field and type your password again. Click **Next**.

If the password does not meet the requirements, the requirement that the password does not meet will be displayed in red. If the **Password** field and **Confirm password** field do not match exactly, the password fields turn red.

Token Registration

Basics

Token registration may require up to three steps:

1. Token insertion ("Token Insertion" on page 12),
2. PIN entry ("Single Sign-On Not Enabled" on page 12),
3. Certificate Selection ("Certificate Selection" on page 13).

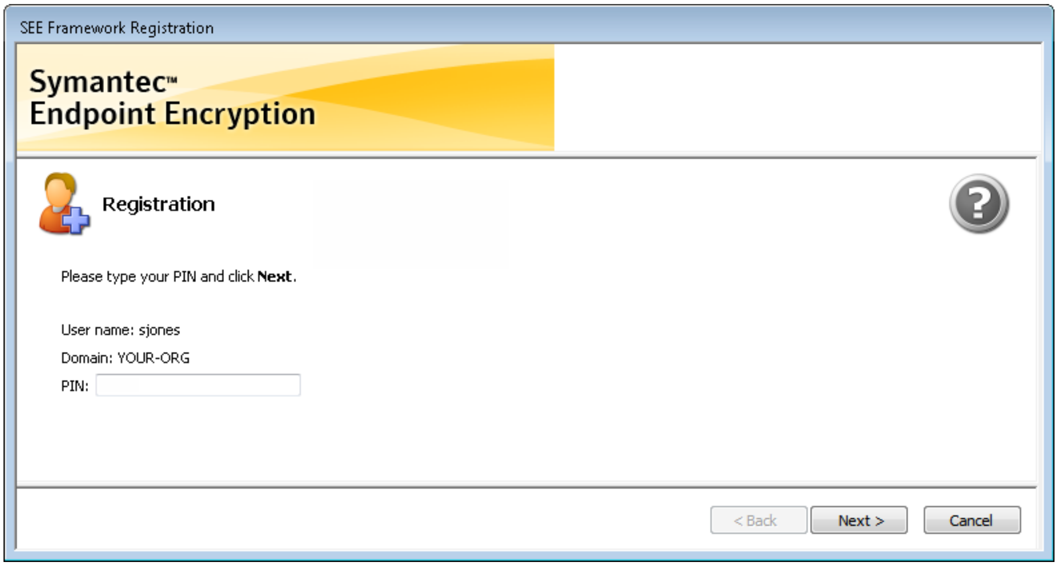
Token Insertion

If your token was inserted when the Registration Wizard began, you do not see a token-insertion prompt panel. Skip to the next section ("Single Sign-On Not Enabled" on page 12).

Otherwise, you will be prompted to insert your token. For details about token insertion and errors, refer to Appendix B "Token Usage & Error Messages" on page 56.

Single Sign-On Not Enabled

If Single Sign-On is not enabled, you will be prompted to type your PIN. If you aren't prompted, skip to the next section "Token Account Credentials" on page 13.



Please type your PIN and click **Next**.

User name: sjones

Domain: YOUR-ORG

PIN:

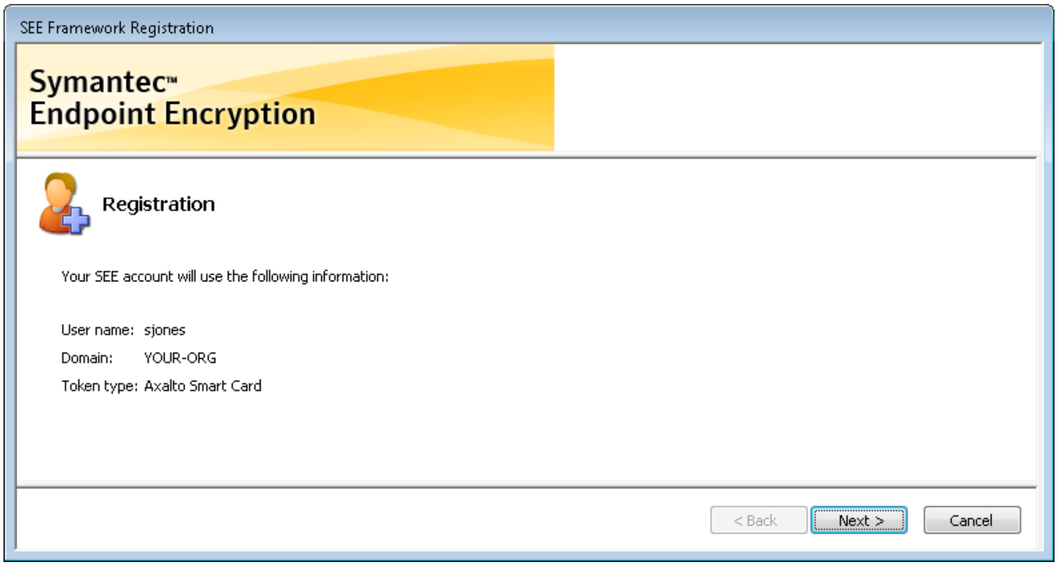
Figure 2.11—Token Registration, Account PIN

The **User name** and **Domain** fields are filled from the information stored on your token.

Type your PIN in the **PIN** field, then click **Next**.

Token Account Credentials

For both SSO and non-SSO accounts, the next registration panel confirms the token information that Symantec Endpoint Encryption will use to authenticate you.



Your SEE account will use the following information:

User name: sjones
Domain: YOUR-ORG
Token type: Axalto Smart Card

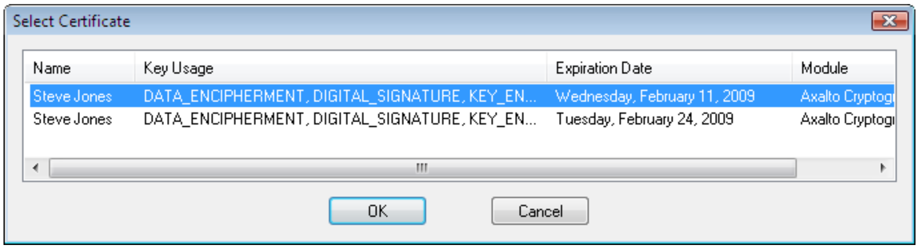
Figure 2.12—Token Registration, Information Summary

For users with Single Sign-On enabled, this information—including your PIN—is your Windows account information.

Verify the information and click **Next**.

Certificate Selection

If the **Select Certificate** window does not appear, skip to “Authenti-Check” on page 14.



Name	Key Usage	Expiration Date	Module
Steve Jones	DATA_ENCIPHERMENT, DIGITAL_SIGNATURE, KEY_EN...	Wednesday, February 11, 2009	Axalto Cryptogr
Steve Jones	DATA_ENCIPHERMENT, DIGITAL_SIGNATURE, KEY_EN...	Tuesday, February 24, 2009	Axalto Cryptogr

Figure 2.13—Select Certificate

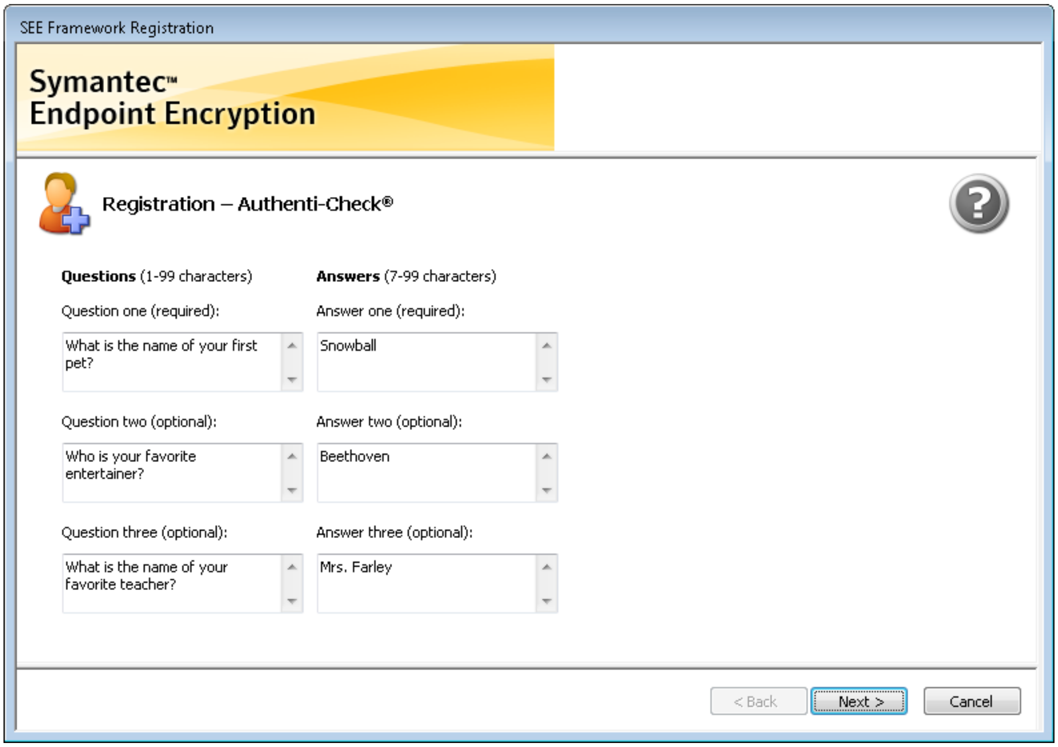
Select your Symantec Endpoint Encryption certificate by clicking on the appropriate row, then click **OK**. Continue to the next section.

If you don’t know which of the certificates listed are valid, contact the appropriate administrator.

If you receive an error message, refer to Appendix B “Error Messages” on page 57.

Authenti-Check

If you have Authenti-Check enabled, then you will see the Authenti-Check panel. If you don't see this panel skip to the next section ("Completion" on page 15).



Registration – Authenti-Check®

Questions (1-99 characters) **Answers** (7-99 characters)

Question one (required): What is the name of your first pet?
Answer one (required): Snowball

Question two (optional): Who is your favorite entertainer?
Answer two (optional): Beethoven

Question three (optional): What is the name of your favorite teacher?
Answer three (optional): Mrs. Farley

Figure 2.14—Registration, Authenti-Check

Authenti-Check is a self-help recovery tool that allows you to gain access to your computer and/or the User Client Console if you forget your password, PIN, or token. It can also be used if you get a new token and need to change tokens.

One Authenti-Check question is always required. Up to three questions may be required, depending on how your system is configured.

Questions identified as required must be entered and answered.

If a question is identified as optional, you are encouraged to enter a question and an answer. The more question-answer pairs you have, the more secure your Full Disk access is. For maximum security, enter three questions and three answers.

Sometimes your Policy Administrator predefines questions for you. These questions you cannot change and you must provide answers for.

Try to choose answers that other people cannot guess easily. Follow similar guidelines for your questions and answers as you would for your password. Create pairs that:

- Do not contain commonly known information,
- Are longer rather than shorter, and
- You can remember without writing down.

See Table 2.1 for examples of secure and less secure questions.

Table 2.1—Authenti-Check Sample Questions

Secure	Less Secure
Who was your favorite teacher?	What is your social security number?
Who was your childhood hero?	Where were you born?
What is the street name where your favorite relative lived?	What is your mother's maiden name?

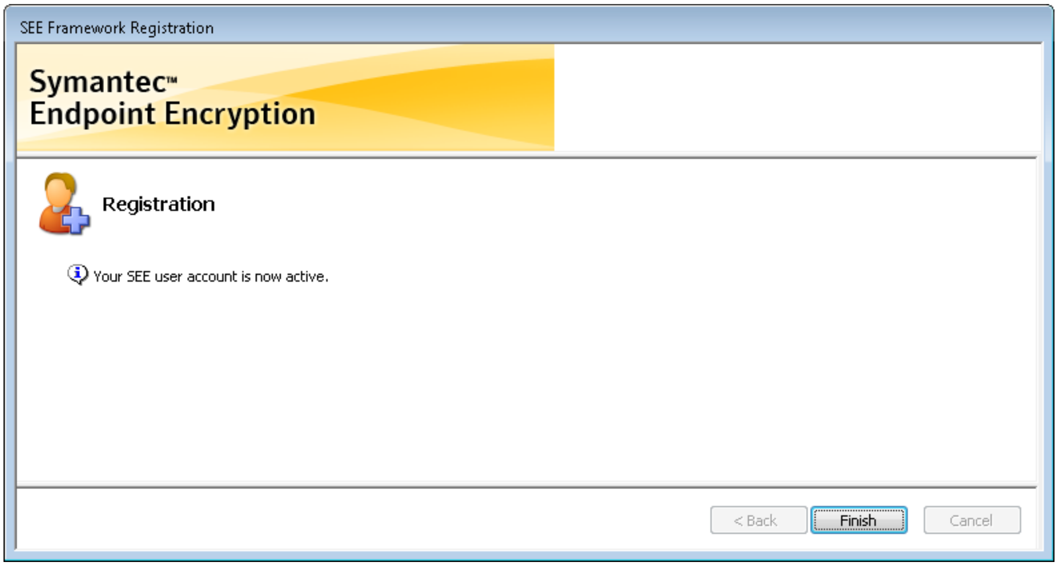
Do not let others watch you enter them. Unlike passwords, the question-answer pairs are not displayed as asterisks or dots on your screen; they display in plain text.

When creating your question/answer pairs, only enter characters that can be typed from the keyboard. Using alternate input methods—such as typing from the ALT+numeric keypad—may create characters that you will not be able to enter in the pre-Windows environment. If you have questions about keyboard use, please ask your Client Administrator.

When you have entered all questions and answers, click the **Next** button to submit your information. If your questions and answers fall within established guidelines, your information will be accepted; otherwise, fields that contain errors are highlighted in red. Correct any highlighted information then click **Next**.

Completion

The final Registration panel notifies you that your Symantec Endpoint Encryption user account is active.



Your SEE user account is now active.

Figure 2.15—Registration Success

Click **Finish** to complete the wizard and dismiss the panel. This will result in the launch of the User Client Console.

See Chapter 5 "User Client Console" on page 34 for information about using the User Client Console.

3. Pre-Windows Authentication

Overview

Basics

Full Disk needs a set of credentials before it allows you to access your protected hard disk. If you have Single Sign-On (SSO), you will log on once with your Windows user name and password or token. If you do not have SSO, you will need to log on to Full Disk and then to Windows. Though it requires an extra step, not having SSO enabled is the more secure configuration.

A third possibility is that your Policy Administrator configured authentication to occur automatically with no intervention from you.

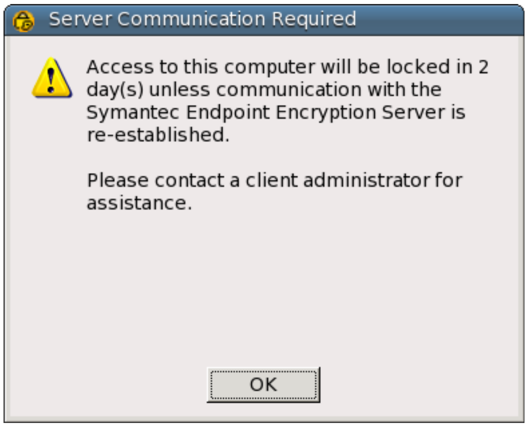
Before powering the computer on, ensure that your keyboard and mouse are connected.

Full Disk provides visually impaired users with audio cues during pre-Windows authentication. Audio cues in the form of system beeps from the computer's internal speaker provide feedback and help guide users to the next action to take when authenticating at the pre-Windows Full Disk logon screen. For instructions on using audio cues, reference Appendix C "Logon Audio Cues" on page 62.

If your computer has a Full Disk check-in policy with lockout enforcement and is not communicating with the Symantec Endpoint Encryption Management Server on the prescribed schedule, you will be locked out of your computer in pre-Windows.

Lockout Warning

If a computer lockout is imminent, a **Server Communication Required** warning message will be displayed immediately after powering on.


Server Communication Required

Access to this computer will be locked in 2 day(s) unless communication with the Symantec Endpoint Encryption Server is re-established.

Please contact a client administrator for assistance.

Figure 3.1—Pre-Windows Logon, Lockout Warning

The number of days varies, based on policy. Click **OK** to dismiss the message.

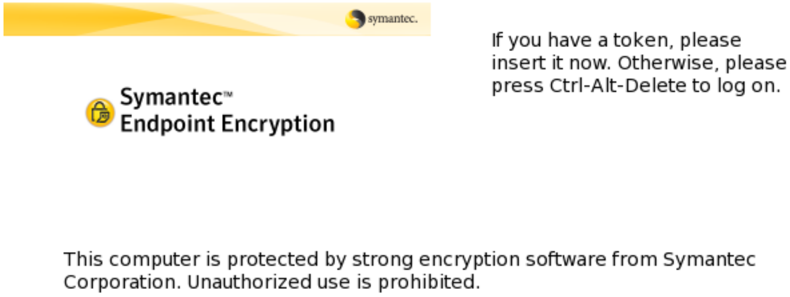
If you are unaware of the reason why your Client Computer is not checking in with the Symantec Endpoint Encryption Management Server, as advised in the message, contact your Client Administrator as soon as possible. They can resolve the problem that is preventing your computer from checking in and/or log on in pre-Windows to prevent the lockout from occurring.

If the problem preventing your computer from checking in is expected—for example, you are running under a virtual private network (VPN) and you are not continually connected—refer to Chapter 5 “Check-In Panel” on page 49 for how to force your computer to check in.

Startup Screen

Once you have registered, each time you turn on your computer, you will be greeted by the Startup screen. The Startup screen may be the default distributed with Full Disk, or it may have been customized by your organization.

The Startup screen and the pre-Windows logon screen may not be displayed if an Autologon policy is in effect. If Autologon is in effect, you will skip the Full Disk logon and log on to Windows only.



If you have a token, please insert it now. Otherwise, please press Ctrl-Alt-Delete to log on.

This computer is protected by strong encryption software from Symantec Corporation. Unauthorized use is prohibited.

Figure 3.2—Startup Screen, Default

If you have the token that you registered with, insert it now. Otherwise, press CTRL+ALT+DEL.

If you need to change the keyboard with which you enter your credentials, continue reading. Otherwise, if you pressed CTRL+ALT+DEL, skip to “Password Logons” on page 18. If you inserted your token, skip to “Token Logons” on page 20.

For details on token insertion, refer to Appendix B “Token Usage” on page 56.

Keyboard Selection

When the pre-Windows Logon screen appears, a keyboard layout bar also appears in the lower right-hand corner of your computer screen.

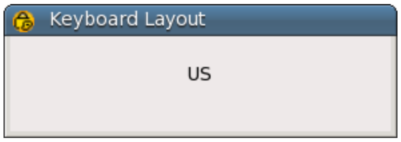


Figure 3.3—Keyboard Layout Bar

If you need a keyboard layout different than the one identified in the bar and your administrator defined multiple keyboards for this computer, use the key sequences listed in Table 3.1 to toggle to another keyboard.

Before toggling, be sure to click on the Keyboard Layout bar, to place the focus there (the title bar becomes dark).

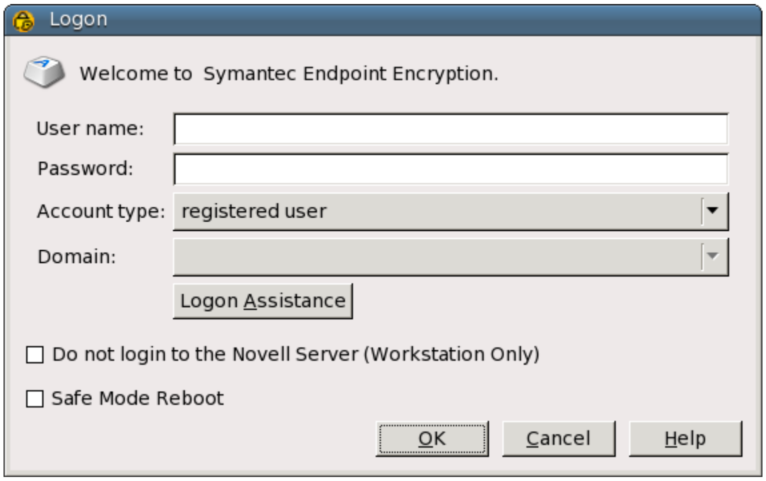
Table 3.1—Pre-Windows Key Sequences for Toggling Among Keyboards

Key Sequence	Toggle To	Description
SHIFT+F6	Default keyboard layout	The default keyboard layout is set up in Windows.
CTRL+F6	US English (101) keyboard layout	The US English keyboard is always available and independent of the Windows layout setup.
F6	Next layout	Press to select the next layout available based on the Windows setup.

Once you have toggled to the desired keyboard, click on the Logon screen.

Password Logons

Once you have pressed CTRL+ALT+DEL, the password Logon screen appears.


Welcome to Symantec Endpoint Encryption.

Account type: registered user

Figure 3.4—Pre-Windows Logon, Password

Type your user name into the **User name** field.

Select your computer name from the **Domain** drop-down menu.

Select **registered user** from the **Account type** drop-down list.

If your administrator has chosen to allow you to start the computer in safe mode, the **Safe Mode Reboot** check box will be displayed. Select the **Safe Mode Reboot** check box if this is a desktop that you want to start in safe mode.

If the Novell Client is installed on your workstation, the **Do not login to the Novell Server (workstation only)** check box will be displayed. This check box is only relevant if Single Sign-On is enabled. Select the **Do not login to the Novell Server (workstation only)** check box if you are experiencing long wait times to get into Windows. The delay could be because your Novell Server is down or unattainable. If the **Do not login to the Novell Server (workstation only)** check box is selected, Full Disk will not attempt to log on to the Novell Server.

The password Logon panel allows to log on with your password, or to obtain logon assistance if you don’t have a password or forgot your password.

If you have a password and know it, type it into the **Password** field and click **OK**. If your account name and password are correct, one of the following will occur:

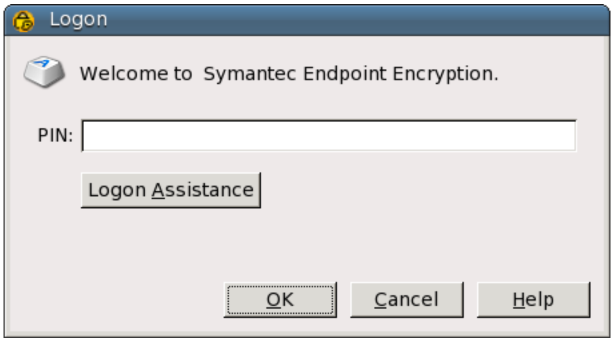
- You will boot directly to Windows if you have SSO.
- If you don’t have SSO, the Windows logon will be displayed.
- If you don’t have SSO, and your password is close to expiring or has expired, you will be prompted to change it before gaining access to the Windows logon.
- If you did not select the **Safe Mode Reboot** check box because you don’t want to start in safe mode, simply wait for Windows to load.
- If you did not select the **Safe Mode Reboot** check box because this is a laptop that you want to start in safe mode, start pressing F8 repeatedly on the internal laptop keyboard.
- If you selected the **Safe Mode Reboot** check box and this is a desktop, a message will be displayed, notifying you that the computer will be restarted to provide you with the safe mode option. Click **Restart Computer**. The computer will restart. The behavior then varies per operating system.
    - On Windows Vista or later, you will be presented with the safe mode option screen.
    - On Windows XP or earlier, you will be presented with an operating system selection screen. Press F8. Then you will be presented with the safe mode option screen.

If your password is incorrect, an error message will be displayed. You may even be forced to wait before you can try again.

If you don’t have a password or forgot your password, click **Logon Assistance**. Skip to Chapter 4 “Pre-Windows Assistance” on page 21.

Token Logons

After inserting your token at the Startup screen, the pre-Windows token Logon screen appears.



Logon

Welcome to Symantec Endpoint Encryption.

PIN:

Figure 3.5—Pre-Windows Logon, Token

Ensure that your token has been recognized (Appendix B “Recognition” on page 56).

- Type your PIN into the **PIN** box and click **OK**.
  - ❑ You will boot directly to Windows if your PIN is correct and you have SSO.
  - ❑ If your PIN is correct and you don’t have SSO, the Windows logon will be displayed.
  - ❑ If your PIN is correct, you don’t have SSO, and you have a Symantec Endpoint Encryption password that is close to expiring or has expired, you will be prompted to change your Symantec Endpoint Encryption password before gaining access to the Windows logon.
  - ❑ If your PIN is incorrect, an error message will be displayed.
- If you forgot your PIN, click **Logon Assistance**. Skip to Chapter 4 “Pre-Windows Assistance” on page 21.

Do not remove your token until processing completes.

If you encounter token, certificate, or PIN errors while trying to log on, refer to Appendix B “Pre-Windows Logon” on page 58 for possible causes and resolution.

4. Pre-Windows Assistance

Overview

Full Disk offers two tools to help you regain access to your computer, should you forget your credentials or get locked out.

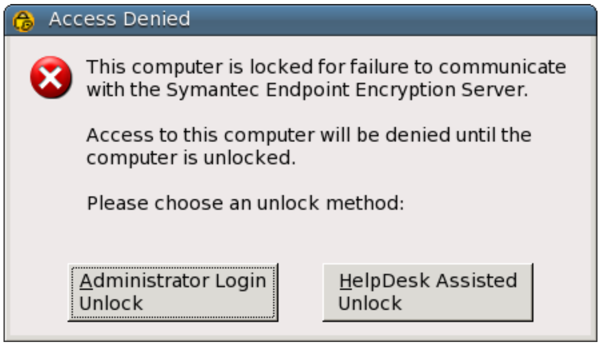
If you get locked out of your computer because it has failed to communicate with the Symantec Endpoint Encryption Management Server, your administrator may have made One-Time Password available to you.

If you forget your password, PIN, or token, your administrator may have provided you with Authenti-Check and/or One-Time Password. These tools are also available in the event that you receive a new token or the certificate on your token is changed.

If you were not provided these tools or they fail to work, you can always contact your Client Administrator.

Lockout Assistance Request

If your computer is locked, the Startup screen will not be displayed after you power on. Instead, you will see an **Access Denied** dialog.



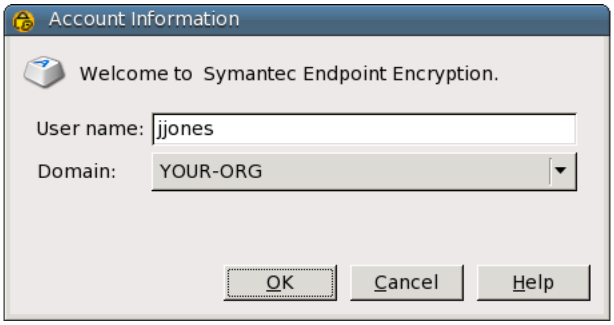
This computer is locked for failure to communicate with the Symantec Endpoint Encryption Server.

Access to this computer will be denied until the computer is unlocked.

Please choose an unlock method:

Figure 4.1—Pre-Windows Logon, Computer Lockout

If you believe you may have been provided with the OTP Communication Unlock feature, click **HelpDesk Assisted Unlock**. The **Account Information** dialog appears.



Welcome to Symantec Endpoint Encryption.

User name: jjones

Domain: YOUR-ORG

Figure 4.2—Pre-Windows Logon, Computer Lockout, Account Information

Type your user name in the **User name** field and select your domain or local computer name from the **Domain** drop-down list. Click **OK**.

If you do not have the feature available, you will be notified. Contact your Client Administrator.

If you do have the feature available, refer to “One-Time Password” on page 27.

Logon Assistance Request

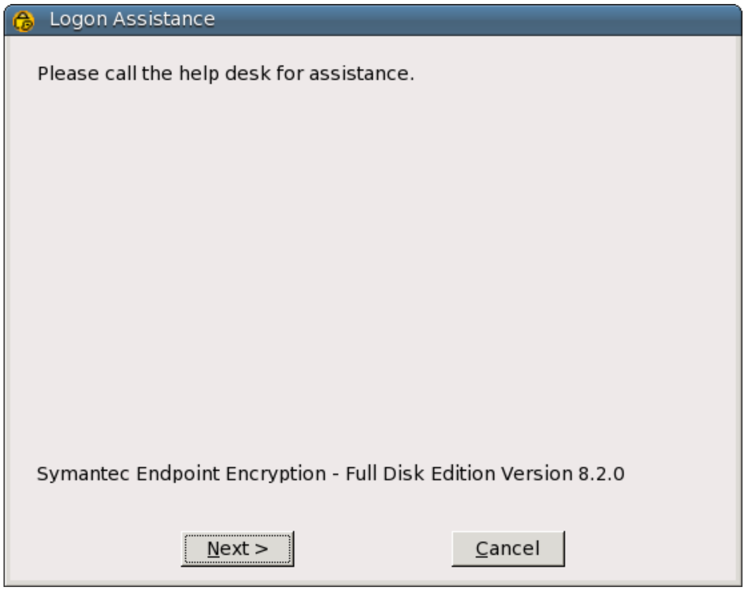
Basics

After clicking **Logon Assistance** from either the password or the token logon, one of the following will occur:

- You will be advised that neither Authenti-Check or One-Time Password is available. Contact your Client Administrator.
- A customizable message will be displayed (“Logon Assistance Features Available” on page 22).

Logon Assistance Features Available

If one or more logon assistance features have been provided, the following window will be displayed.



Please call the help desk for assistance.

Symantec Endpoint Encryption - Full Disk Edition Version 8.2.0

Figure 4.3—Pre-Windows Logon Assistance, Logon Assistance Features Available

The text within this window is customized by your administrator. It should provide you with instructions as to how to contact the help desk.

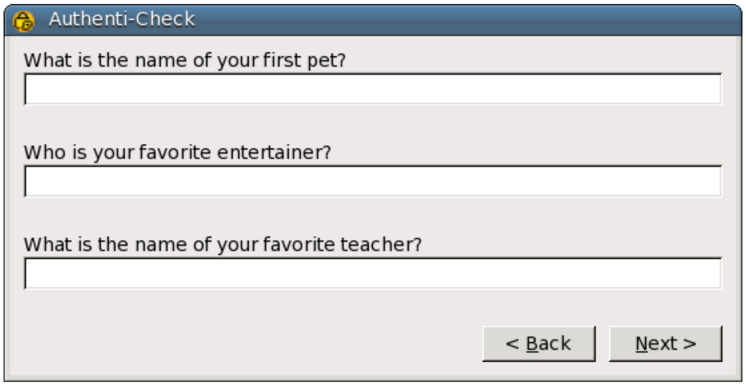
Authenti-Check

Basics

The logon assistance will begin with Authenti-Check, if you have Authenti-Check available. If the Authenti-Check window does not display, skip to “One-Time Password” on page 27.

Prompts

Authenti-Check will begin by asking you the answers to the questions that you pre-established.



Authenti-Check

What is the name of your first pet?

Who is your favorite entertainer?

What is the name of your favorite teacher?

Figure 4.4—Pre-Windows Logon Assistance, Authenti-Check

Authenti-Check involves up to three question-answer pairs, established during Symantec Endpoint Encryption registration.

In each box that appears below a question, type the correct answer. Make sure that you enter the answer exactly as you entered it when you defined it. Note that punctuation matters. The answers are not case-sensitive.

If an Authenti-Check answer is long (up to 99 characters may be allowed by policy), the characters that you type at the beginning of the answer may move out of view as you continue to type. You can press the arrow keys or HOME and END keys to scroll through your answer, or you can use SHIFT in combination with arrow keys to select text.

If you need to delete some or all of the text of a long answer, use one of the methods below to ensure that the non-visible characters are deleted:

- To delete the entire answer, press END, then SHIFT+HOME. All text becomes highlighted. Press DELETE.
- To delete part of the answer, use an arrow key to move to the right of the characters in question, then press BACKSPACE until all of the characters that you intended to delete are removed. You could also move to the left of the characters, then press DELETE.

Replace any deleted text with correct information, as appropriate.

Once you have entered your answers, click **Next**. Go to the appropriate section:

- “Success, Token-Only User” on page 23
- “Success, User with Symantec Endpoint Encryption Password, SSO Enabled” on page 24,
- “Success, User with Symantec Endpoint Encryption Password, SSO Not Enabled” on page 25,
- “Failure, OTP Not Enabled” on page 26, or
- “Failure, OTP Enabled” on page 27.

Success, Token-Only User

If the Authenti-Check process ends successfully and SSO is enabled, Windows will proceed to load. If SSO is not enabled, you are prompted to authenticate to Windows.

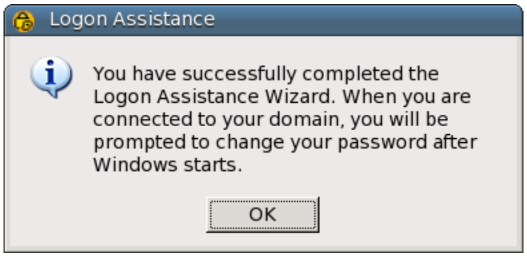
Once Windows loads, you should take one of the following actions:

- If you have forgotten your PIN, contact the appropriate administrator.

- If you have forgotten your token or have a new token, the User Client Console will launch automatically once Windows loads. If you have a new token, use Authenti-Check to gain access to the User Client Console (Chapter 5 “Authentication Assistance” on page 37). Open the Token panel. Follow the instructions displayed on the Token panel (Chapter 5 “Token Panel” on page 44).

Success, User with Symantec Endpoint Encryption Password, SSO Enabled

If you have a Symantec Endpoint Encryption password, the Authenti-Check process ends successfully, and SSO is enabled, a logon assistance success message is displayed.


Logon Assistance

You have successfully completed the Logon Assistance Wizard. When you are connected to your domain, you will be prompted to change your password after Windows starts.

Figure 4.5—Pre-Windows Logon Assistance, SSO Success

You should be prompted to change your Windows password before gaining access to Windows.

The prompt will vary slightly, depending on the version of Windows you are using and whether or not you are using Novell. Enter your new password into the **New password** field. Type your password again, in the **Confirm password** field. Press ENTER.

If your password is not valid, Windows displays an error message. Correct your information and press ENTER again.

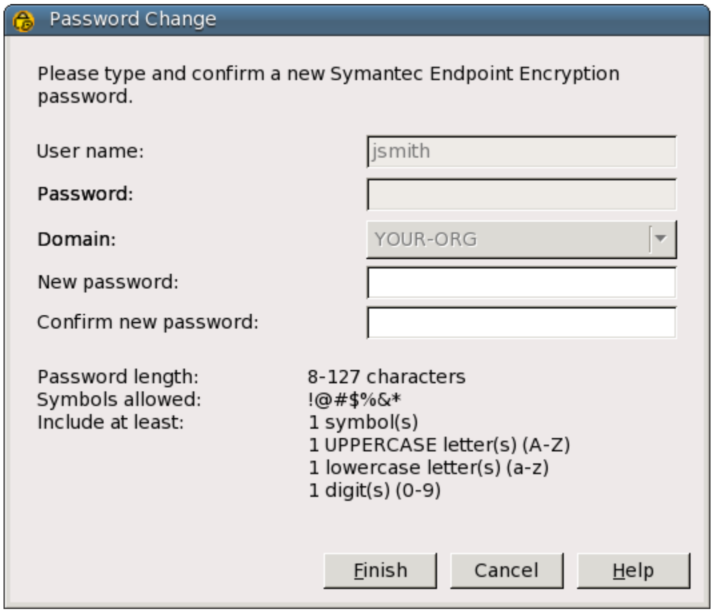
If your password satisfies all Windows password requirements and if the new password and confirmed password match, your Windows password is changed and you gain access to Windows. The next time you log on in pre-Windows, use the new password.

If your Windows account is new or you changed your Windows password quite recently, Windows may stop you from changing your password again because of a minimum password-age restriction. If this happens, call your help desk. Your system administrator will need to reset your Windows password.

If you are a domain user and are not connected to your network, you will not be prompted to change your password. Contact the appropriate administrator to regain your network access.

Success, User with Symantec Endpoint Encryption Password, SSO Not Enabled

If you have a Symantec Endpoint Encryption password, the Authenti-Check process ends successfully, and SSO is not enabled, the Symantec Endpoint Encryption **Password Change** dialog appears.



Please type and confirm a new Symantec Endpoint Encryption password.

User name: jsmith

Password:

Domain: YOUR-ORG

New password:

Confirm new password:

Password length: 8-127 characters
Symbols allowed: !@#$%&*
Include at least: 1 symbol(s)
1 UPPERCASE letter(s) (A-Z)
1 lowercase letter(s) (a-z)
1 digit(s) (0-9)

Figure 4.6—Symantec Endpoint Encryption Password Change Prompt

Enter a new password in the **New password** box. Follow any requirements shown on the dialog box for **Password length**, **Symbols allowed**, and **Include at least**.

Symbols allowed identifies which of the non-alphanumeric characters on your keyboard may be included in the password.

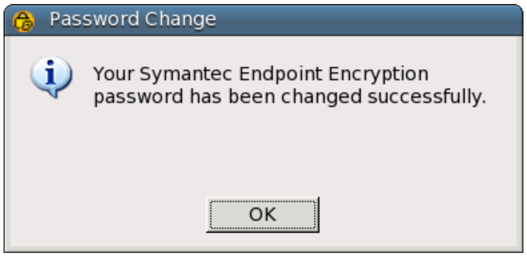
Include at least displays the number of required symbols, uppercase letters, lowercase letters, and/or digits that your password must contain, if any.

When creating your password, only enter characters that can be typed from the keyboard. Using alternate input methods—such as typing from the ALT+numeric keypad—may create characters that you will not be able to enter in the pre-Windows environment. If you have questions about keyboard use, please ask your Client Administrator.

Type your new password again, in the **Confirm new password** box.

Click **Finish**. Your password is submitted.

If the password meets the requirements and the confirmation matches, a **Password Change** success message appears.



Password Change

Your Symantec Endpoint Encryption password has been changed successfully.

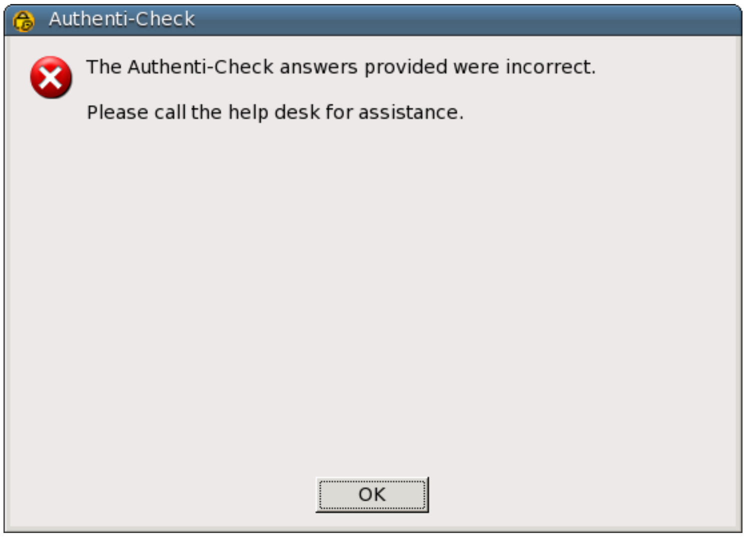
Figure 4.7—Symantec Endpoint Encryption Password Change Success

Click **OK** to dismiss the message.

Once your password is changed, Windows loads. If your password is not valid, an error message appears. Re-enter the information and click **Finish** again.

Failure, OTP Not Enabled

If your Authenti-Check answers are not correct, a message box appears with an error message and instructions on what to do next.



Authenti-Check

The Authenti-Check answers provided were incorrect.

Please call the help desk for assistance.

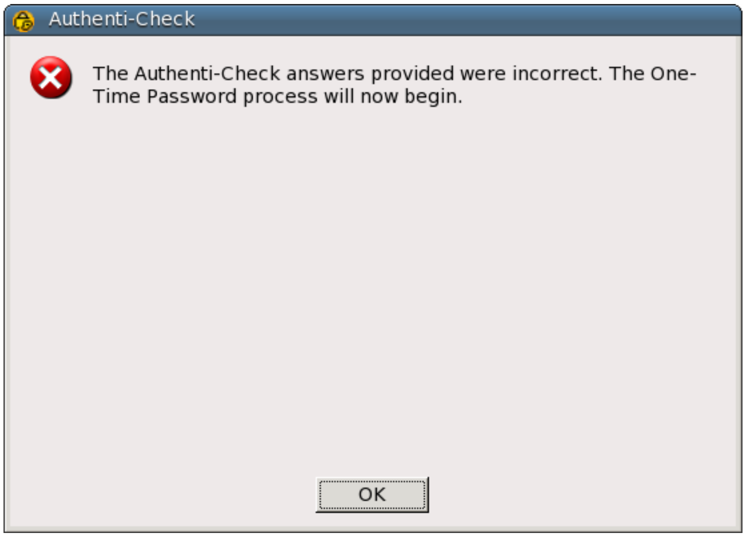
Figure 4.8—Pre-Windows Logon Assistance, Authenti-Check Failure, No OTP

Your instructions may differ from the instructions shown in Figure 4.8 if your Policy Administrator customized them.

Click **OK.** You return to the password Logon screen (Figure 3.4). Call your Client Administrator for help.

Failure, OTP Enabled

If OTP is enabled, after a failed Authenti-Check attempt, you will see a message advising you that OTP is about to begin.



The Authenti-Check answers provided were incorrect. The One-Time Password process will now begin.

Figure 4.9—Pre-Windows Logon Assistance, Authenti-Check Failure, OTP Begins

Click **OK**.

One-Time Password

Basics

The One-Time Password (OTP) Program allows you to obtain:

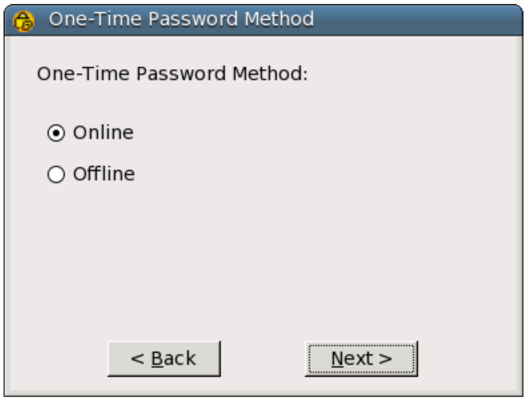
- Logon assistance for a forgotten password, PIN, or token, and/or
- Computer lockout assistance, if allowed by policy.

OTP provides you with a one-time password—known as a response key—that allows you to authenticate temporarily. If you are recovering from a forgotten password, you will be prompted to enter a new password when Windows loads.

Make contact with your Policy Administrator before you begin.

Method Selection

First, you will be prompted to select your OTP method.


One-Time Password Method

One-Time Password Method:

● Online

○ Offline

Figure 4.10—Pre-Windows Assistance, OTP Method Selection

Accept the default selection unless you are advised otherwise by your Policy Administrator and click **Next**.

If you will be using the offline method, see the section “Offline Method” on page 30.

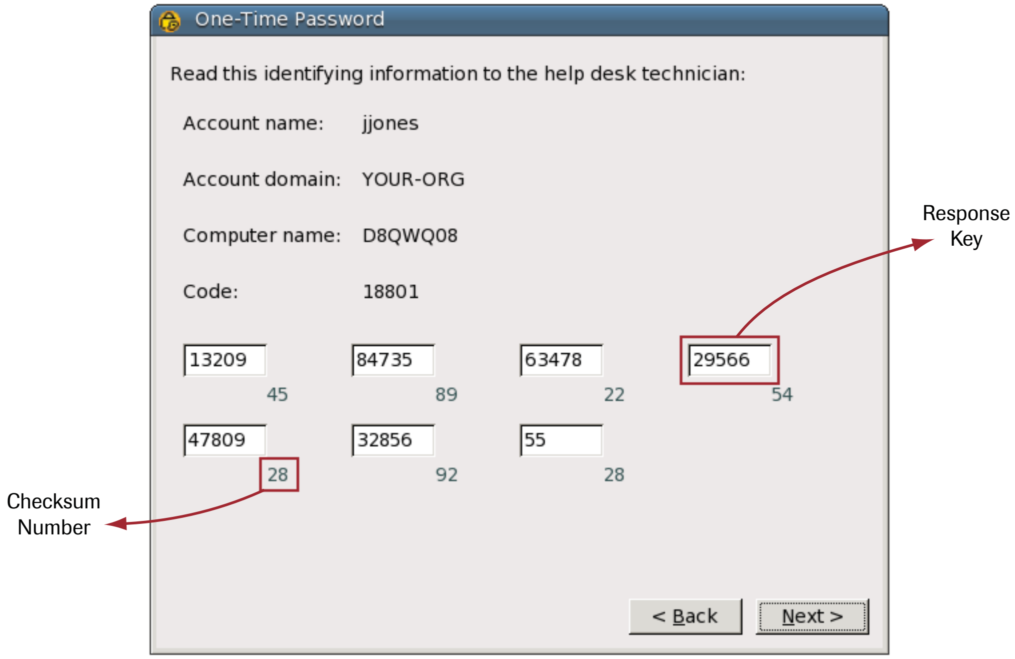
If you will be using the online method, continue to the next section.

Online Method

If **Online** was selected, the One-Time Password screen appears, with the **Account name**, **Account domain**, and **Computer name** fields displaying your Symantec Endpoint Encryption user name, domain, and computer name, respectively. In addition, a **Code** is displayed. The response key fields are blank.

Tell the Policy Administrator the **Account name**, **Account domain**, **Computer name**, and **Code** information displayed in your window.

The Policy Administrator will then provide the response key.



One-Time Password

Read this identifying information to the help desk technician:

Account name: jjones

Account domain: YOUR-ORG

Computer name: D8QWQ08

Code: 18801

13209 45	84735 89	63478 22	29566 54
47809 28	32856 92	55 28	

Response Key

Checksum Number

Figure 4.11—Pre-Windows Assistance, OTP Online

Type the response key numbers into the fields on your screen. Enter the numbers in sequence, from left to right and top to bottom.

After you have entered the response key numbers, the Policy Administrator may ask you to provide the checksums that appear to the bottom-right of each data-entry field. These checksums confirm that you have entered the numbers correctly. A matching checksum quickly verifies that all of the digits from the first box up to and including the box with the checksum you are confirming are correct. Figure 4.11 shows an example with callouts that identify a response key number and a checksum number.

If the Policy Administrator confirms that the numbers you entered are correct, click **Next**.

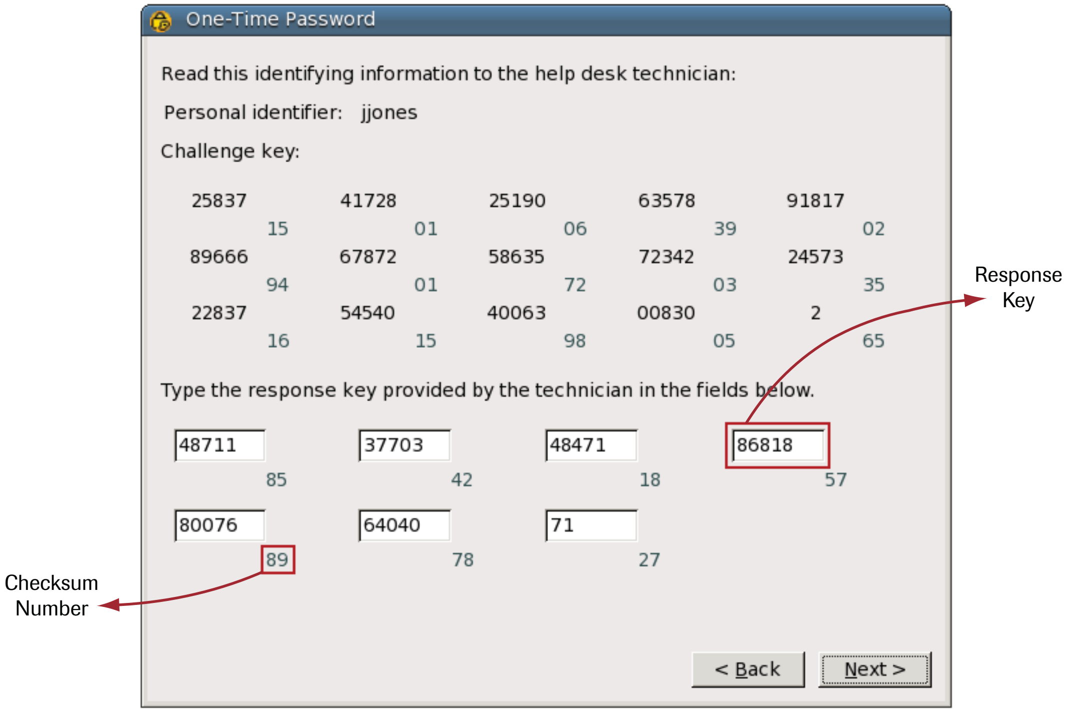
The Policy Administrator will ask you if the method succeeded or failed. If the online method fails, you will begin the offline method. Skip to the next section.

If the online method succeeds, the subsequent steps will differ according to whether you requested assistance for missing credentials or to recover from a lockout condition.

- If you were missing your credentials, refer to the section that matches your authentication method:
  - ❑ “Token-Only User” on page 31,
  - ❑ “User with Symantec Endpoint Encryption Password, SSO Enabled” on page 31, or
  - ❑ “User with Symantec Endpoint Encryption Password, SSO Not Enabled” on page 32.
- If you were locked out of your computer for a failure to communicate, the Windows logon will be displayed.

Offline Method

The One-Time Password challenge/response key screen launches.



One-Time Password

Read this identifying information to the help desk technician:

Personal identifier: jjones

Challenge key:

25837	41728	25190	63578	91817
15	01	06	39	02
89666	67872	58635	72342	24573
94	01	72	03	35
22837	54540	40063	00830	2
16	15	98	05	65

Type the response key provided by the technician in the fields below.

48711	37703	48471	86818
85	42	18	57
80076	64040	71	
89	78	27	

Figure 4.12—Pre-Windows Assistance, OTP Offline

Tell your Policy Administrator the **Personal identifier** that is displayed on your window.

The Policy Administrator will ask you to tell him or her the challenge key numbers. Provide the numbers from left to right and top to bottom. The Policy Administrator may ask you to provide the checksums that appear to the bottom-right of each data-entry field. These checksums confirm that the Policy Administrator has correctly entered the numbers you have provided. A matching checksum quickly verifies that all of the digits from the first box up to and including the box with the checksum you are confirming guarantees that all of the digits up to that box are correct.

The Policy Administrator will then provide the response key.

Type the response key numbers into the blank fields on your screen. Enter the numbers in sequence, from left to right and top to bottom.

After you have entered the response key numbers, the Policy Administrator may ask you to provide the checksums that appear to the bottom-right of each data-entry field. These checksums confirm that you have entered the numbers correctly. As with the challenge key verification, a matching checksum quickly verifies that all of the digits from the first box up to and including the box with the checksum you are confirming are correct. Figure 4.12 shows an example with callouts that identify a response key number and a checksum number.

If the Policy Administrator confirms that the numbers you entered are correct, click **Next**.

The Policy Administrator will ask you if the method succeeded or failed. If the method failed, your Policy Administrator may ask you to try the method again.

If you are using the offline method, after you click **Next** on the final screen, the subsequent steps will differ according to whether you requested assistance for missing credentials or to recover from a lockout condition.

- If you were missing your credentials, refer to the section that matches your authentication method:
    - ❑ "Token-Only User" on page 31,
    - ❑ "User with Symantec Endpoint Encryption Password, SSO Enabled" on page 31, or
    - ❑ "User with Symantec Endpoint Encryption Password, SSO Not Enabled" on page 32.
- If you were locked out of your computer for a failure to communicate, the Windows logon will be displayed.

Success for Missing Credentials

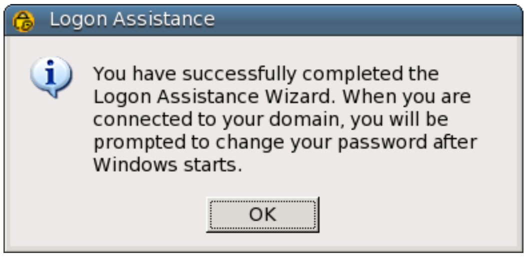
Token-Only User

If the OTP process ends successfully and SSO is enabled, Windows will proceed to load. If SSO is not enabled, you are prompted to authenticate to Windows.

Once Windows loads, the User Client Console will launch. If you have a new token, use Authenti-Check to gain access to the User Client Console. Then open the Token panel to update your account with the new token.

User with Symantec Endpoint Encryption Password, SSO Enabled

If the OTP process ends successfully and SSO is enabled, Windows proceeds to load. The message shown in Figure 4.13 appears:



You have successfully completed the Logon Assistance Wizard. When you are connected to your domain, you will be prompted to change your password after Windows starts.

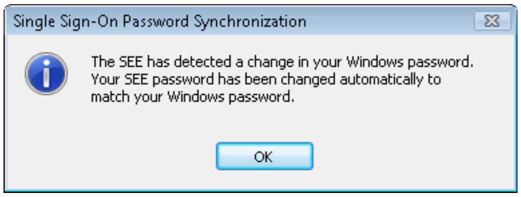
Figure 4.13—Pre-Windows Logon Assistance, SSO Password Change Success

You should be prompted to change your Windows password before gaining access to Windows.

The prompt will vary slightly, depending on the version of Windows you are using and whether or not you are using Novell. Type and confirm your new password, then submit the information.

If your password is not valid, an error message will be displayed. Correct your information and submit it again.

If your password satisfies all Windows password requirements and if the new password and confirmed password match, your Windows password is changed and you gain access to Windows. Symantec Endpoint Encryption then displays a message informing you that your Windows password and your Symantec Endpoint Encryption password have been automatically synchronized.



Single Sign-On Password Synchronization

The SEE has detected a change in your Windows password. Your SEE password has been changed automatically to match your Windows password.

Figure 4.14—Single Sign-On Password Synchronization for Windows

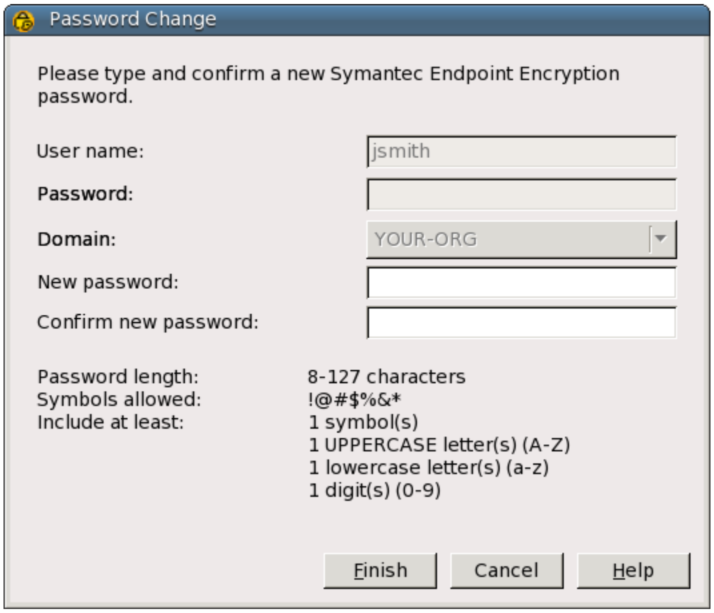
The next time you log on in pre-Windows, use the new password.

If your Windows account is new or you changed your Windows password quite recently, Windows may stop you from changing your password again because of a minimum password-age restriction. If this happens, call your help desk. Your system administrator will need to reset your Windows password.

If you are a domain user and are not connected to your network, you will not be prompted to change your password. Contact the appropriate administrator to regain your network access.

User with Symantec Endpoint Encryption Password, SSO Not Enabled

If your OTP process ends successfully and SSO is not enabled, the Symantec Endpoint Encryption **Password Change** dialog appears.



Password Change

Please type and confirm a new Symantec Endpoint Encryption password.

User name: jsmith

Password:

Domain: YOUR-ORG

New password:

Confirm new password:

Password length: 8-127 characters
Symbols allowed: !@#$%&*
Include at least: 1 symbol(s)
1 UPPERCASE letter(s) (A-Z)
1 lowercase letter(s) (a-z)
1 digit(s) (0-9)

Figure 4.15—Symantec Endpoint Encryption Password Change Prompt

Enter a new password in the **New password** field. Follow any requirements shown on the dialog box for **Password length**, **Symbols allowed**, and **Include at least**.

Symbols allowed identifies which of the non-alphanumeric characters on your keyboard may be included in the password.

Include at least displays the number of required symbols, uppercase letters, lowercase letters, and/or digits that your password must contain, if any.

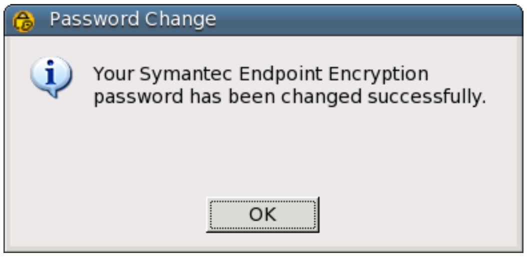
When creating your password, only enter characters that can be typed from the keyboard. Using alternate input methods—such as typing from the ALT+numeric keypad—may create characters that you will not be able to enter in the pre-Windows environment. If you have questions about keyboard use, please ask your Client Administrator.

Type your new password again in the **Confirm new password** field.

Click **Finish**. Your password is submitted.

If your password is not valid, an error message appears. Re-enter the information and click **Finish** again.

If the password meets the requirements and the confirmation matches, a password-change success message appears.



Your Symantec Endpoint Encryption password has been changed successfully.

Figure 4.16—Symantec Endpoint Encryption Password Change Success

Once your password is changed, Windows loads.

5. User Client Console

Overview

The User Client Console is available in Windows and allows you to:

- View the encryption status of your hard disk partitions.
- View the Symantec Endpoint Encryption registered user accounts on your computer.
- View the last time your computer checked in with the Symantec Endpoint Encryption Management Server, if at all.
- View product version information.
- Encrypt non-Opal compliant drives.

In addition, you might be able to:

- Add or change a Symantec Endpoint Encryption password.
- Add or change a token.
- Add or change your Authenti-Check questions and answers.
- Force your computer to check in with the Symantec Endpoint Encryption Management Server.
- Decrypt drives encrypted by Symantec Endpoint Encryption Full Disk.
- View, set, or reset your Novell account information.

These additional functions may or may not have been enabled by your Policy Administrator.

This chapter begins by describing how to start, log on to, and navigate the User Client Console. The chapter then describes step-by-step instructions for doing the tasks listed above.

To start the User Client Console, on the **Start** menu, click **All Programs**, click **Symantec Endpoint Encryption Client**, and then click **Symantec Endpoint Encryption Client**.

- The Logon panel appears (“Logon Panel” on page 35), if SSO is not enabled. If SSO is enabled, the Logon panel also appears if this is the first time that you are launching the User Client Console in this Windows session, or if you chose to log off of your Symantec Endpoint Encryption session the last time you exited the User Client Console.
- The Home panel appears (“Home Panel” on page 40), if SSO is enabled and you are subsequently launching the User Client Console after choosing not to log off of your Symantec Endpoint Encryption session the last time you exited the User Client Console.
- You will be prompted to register, if you have not already done so (Chapter 2 “Registration & Re-Registration” on page 4).
- You will be advised that all user account slots have been taken and you cannot register. Contact your Client Administrator.

The User Client Console will be launched automatically under the following circumstances:

- Following registration, to encourage you to review your settings.
- Following the application of new Authenti-Check policies, to encourage you to update or set your questions and answers.

If Single Sign-On is enabled, when you click the close button ☒ on the User Client Console, you will be asked whether you want to log off of your Symantec Endpoint Encryption session. If you click **Yes**, the next time you launch the User Client Console, you will need to authenticate. If you click **No**, you will be able to launch the User Client Console any number of times during this Windows session without authenticating again.

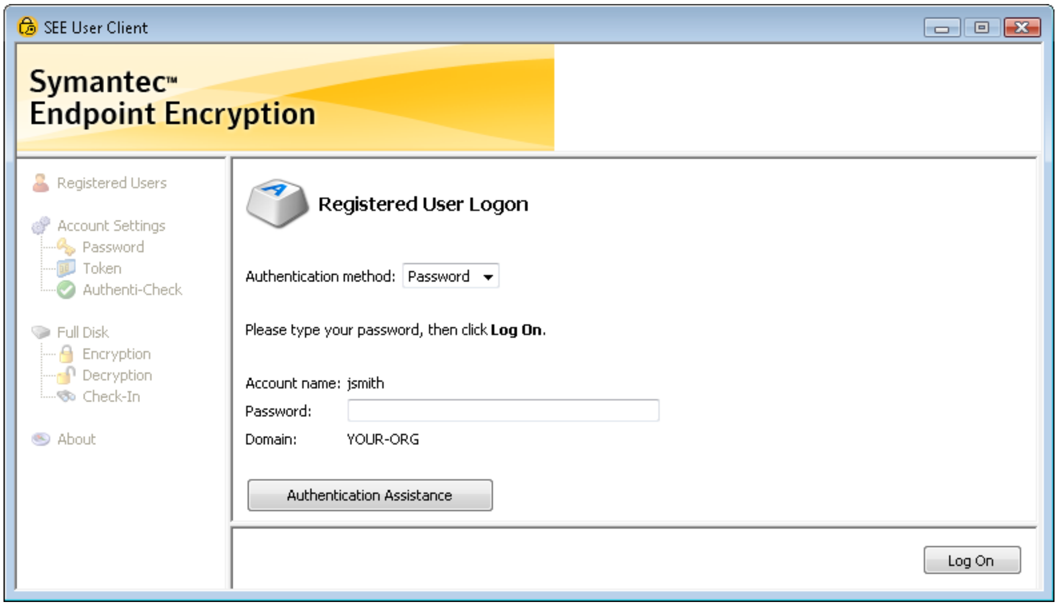
Logon Panel

Basics

Only the user currently logged on to Windows can authenticate to the User Client Console. For password logons, continue to the next section. For token logons, skip to “Token Logon” on page 36. For logon assistance, skip to “Authentication Assistance” on page 37.

Password Logon

If you have a Symantec Endpoint Encryption password, you can use it to log on to the User Client Console.



Registered User Logon

Authentication method: Password

Please type your password, then click **Log On**.

Account name: jsmith
Password:
Domain: YOUR-ORG

Figure 5.1—User Client Console Logon, Password

The **Authentication Method** drop-down list will only be displayed if you are allowed to authenticate with either a password or a token and you have defined both. To log on to the User Client Console with a password, ensure that **Password** is selected from the **Authentication Method** drop-down list.

Type your Symantec Endpoint Encryption password in the **Password** field, then click **Log On**.

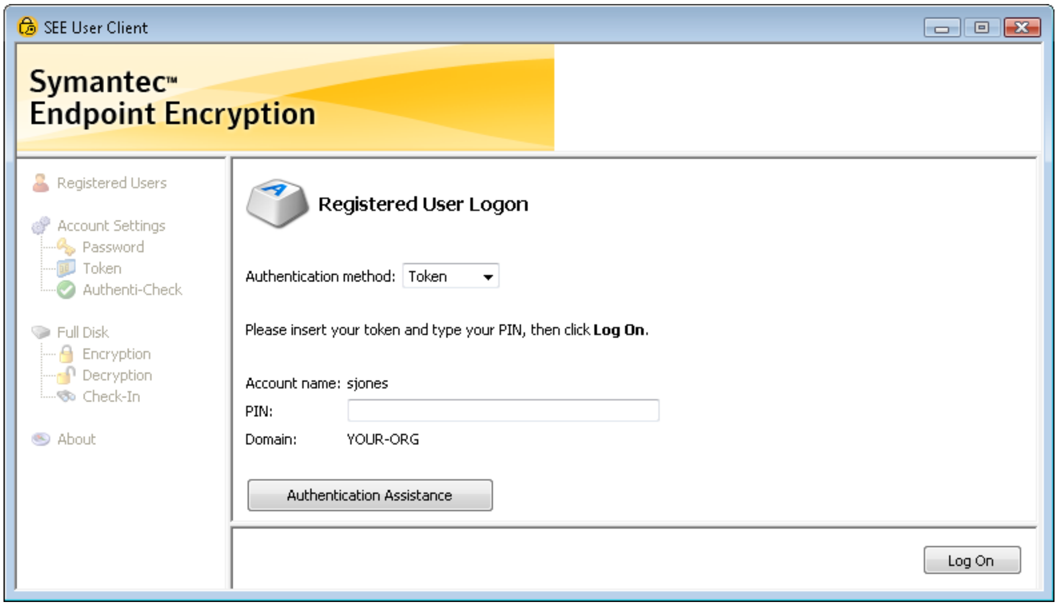
If your password is not correct, the logon fails. Check your password and re-enter the information.

You may be forced to wait before you can log on. Logon delays protect against automated password-guessing attacks. The length of the delay and the maximum number of incorrect logon attempts are set by your administrator.

If your password is correct, you are given access to the User Client Console. Skip to “Home Panel” on page 40.

Token Logon

If you registered with a token or you added a token, you can use it to log on to the User Client Console.



Authentication method: Token

Please insert your token and type your PIN, then click **Log On**.

Account name: sjones

PIN:

Domain: YOUR-ORG

Figure 5.2—User Client Console Logon, Token

The **Authentication Method** drop-down list will only be displayed if you are allowed to authenticate with either a password or a token and you have defined both. Select **Token** from the **Authentication Method** drop-down list.

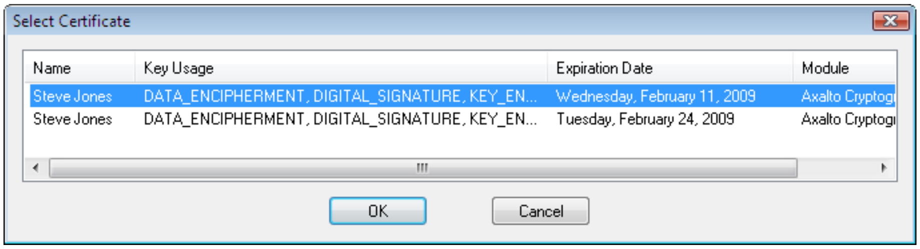
If your token is not already inserted, insert it now. For detailed instructions on token insertion, refer to Appendix B “Token Usage & Error Messages” on page 56.

In the **PIN** field, type your PIN, then click **Log On**. Do not remove the token until authentication completes.

If your authentication succeeds, you are given access to the User Client Console. Skip to the section “Home Panel” on page 40.

If your authentication fails or you encounter token, certificate, or PIN errors during logon, refer to Appendix B “Token Usage & Error Messages” on page 56 for possible causes and resolution.

If the **Select Certificate** dialog appears, continue reading; otherwise, skip to the next section “Home Panel” on page 40.



Name	Key Usage	Expiration Date	Module
Steve Jones	DATA_ENCIPHERMENT, DIGITAL_SIGNATURE, KEY_EN...	Wednesday, February 11, 2009	Axalto Cryptog
Steve Jones	DATA_ENCIPHERMENT, DIGITAL_SIGNATURE, KEY_EN...	Tuesday, February 24, 2009	Axalto Cryptog

Figure 5.3—Select Certificate

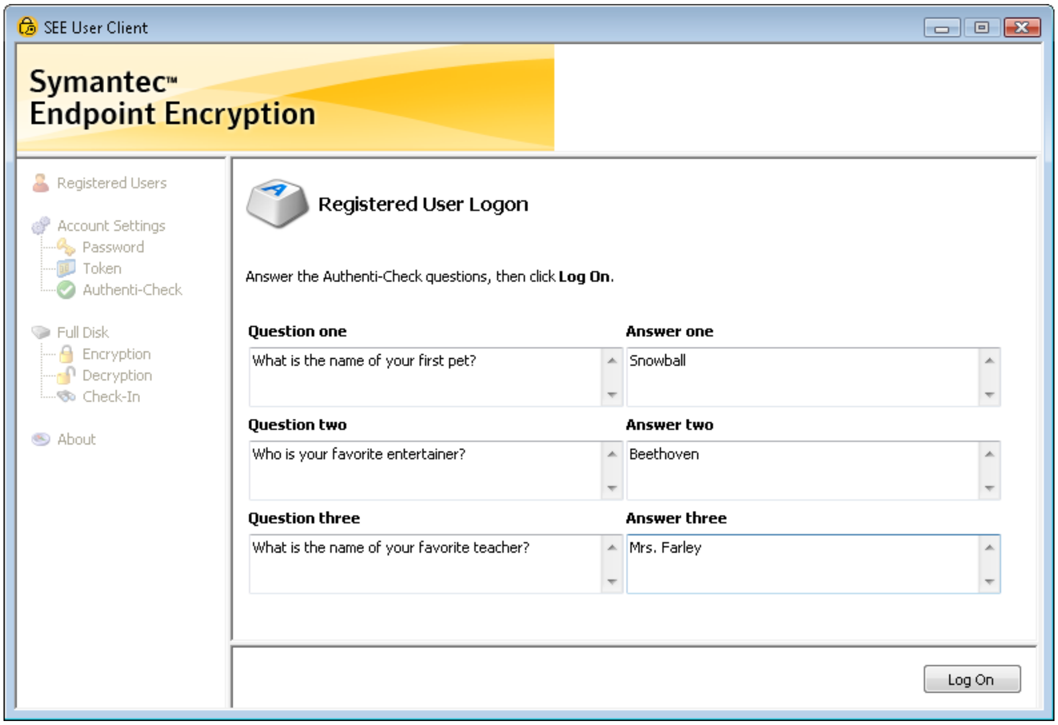
Select your Symantec Endpoint Encryption certificate by clicking on the appropriate row, then clicking **OK**. In the Figure 5.3 example, the token administrator created two certificates with the expected key usage settings, so this user identifies their certificate based on expiration date.

If you don’t know which certificate to choose, contact your token administrator or your Client Administrator.

If you receive an error message, refer to Appendix B “Token Usage & Error Messages” on page 56 for possible causes and resolution.

Authentication Assistance

If you have Authenti-Check enabled for your account, the **Authentication Assistance** button will be available from the Logon panel. Click **Authentication Assistance** if you forgot or do not have the credentials associated with your account.



Registered User Logon

Answer the Authenti-Check questions, then click **Log On**.

Question one	Answer one
What is the name of your first pet?	Snowball
Question two	**Answer two**
Who is your favorite entertainer?	Beethoven
Question three	**Answer three**
What is the name of your favorite teacher?	Mrs. Farley

Figure 5.4—User Client Console Logon, Authenti-Check

Authenti-Check involves up to three question-answer pairs, established during Symantec Endpoint Encryption registration.

In each box that appears beside a question, type the correct answer. Make sure that you enter the answer exactly as you entered it when you defined it. Note that punctuation matters. The answers are not case-sensitive.

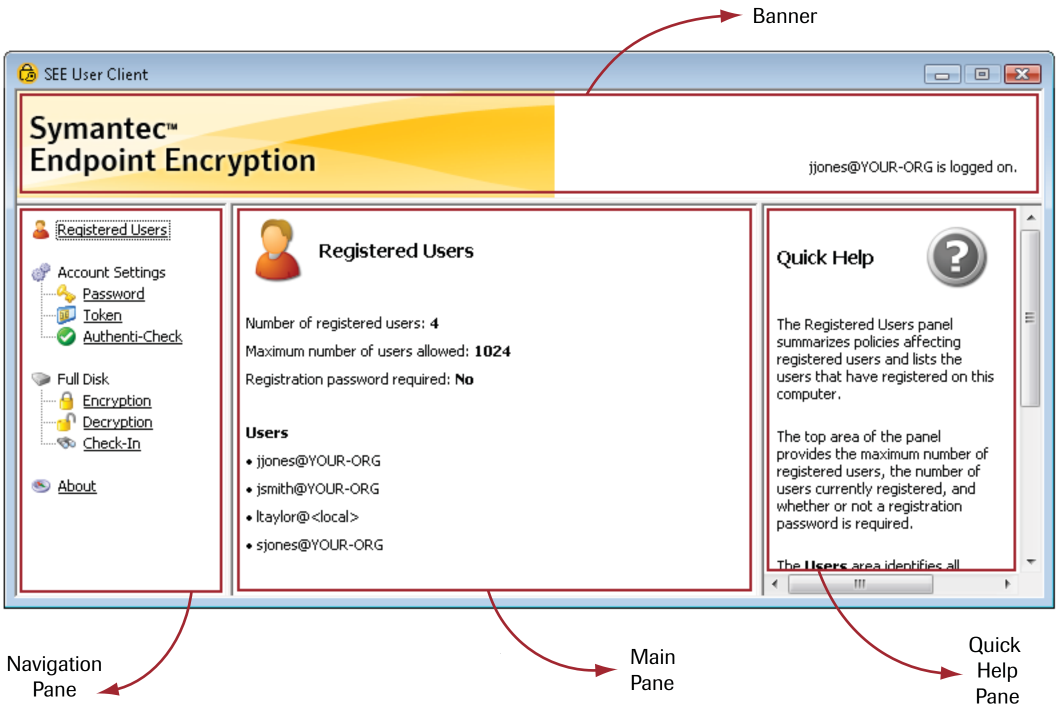
Once you have entered your answers, click **Log On**. One of the following will result:

- The Home panel will be displayed.
- You will be advised that your answers were incorrect.
- You will be advised that your answers were incorrect and forced to wait before you can try again.

Navigation

User Interface Elements

The User Client Console is divided into several sections.



jjones@YOUR-ORG is logged on.

Registered Users

Number of registered users: **4**

Maximum number of users allowed: **1024**

Registration password required: **No**

Users

- jjones@YOUR-ORG
- jsmith@YOUR-ORG
- ltaylor@<local>
- sjones@YOUR-ORG

Quick Help

The Registered Users panel summarizes policies affecting registered users and lists the users that have registered on this computer.

The top area of the panel provides the maximum number of registered users, the number of users currently registered, and whether or not a registration password is required.

The **Users** area identifies all

Figure 5.5—User Client Console User Interface Elements

The sections are as follows:

- The banner displays the product logo, the name of the currently logged on user, and the user’s domain or local computer name.
- The navigation pane contains hyperlinks to all panels. A panel loads into the main pane when its link is clicked.
- The main pane changes in response to your clicking a link in the navigation pane. For example, if you click *Registered Users*, the main pane displays the Registered Users panel.

Standard visual indicators are used to identify the user interface element that has focus. A dotted line outlines the link, button, check box, or icon having focus. Highlighting or a blinking cursor indicates the input field that has focus. In Figure 5.5, *Registered Users* has focus.

You can navigate the User Client Console using a mouse or using the keyboard.

Mouse Navigation

If you are using a mouse:

- To load a panel, click the desired hyperlink in the navigation pane; the panel loads into the main pane.
- To display Quick Help, click the help icon ?. The Quick Help pane appears. To close the Quick Help pane, click the help icon again.

Keyboard Navigation

Direct Access

Use the keys listed in the following table to directly access User Client Console panels.

Table 5.1—Access Keys

To Go To This Panel		Press This Key
Registered Users		ALT+U
Account Settings	Password	ALT+P
	Token	ALT+K
	Authenti-Check	ALT+A
Full Disk	Encryption	ALT+E
	Decryption	ALT+D
	Check-In	ALT+C
	Novell SSO	ALT+N
About		ALT+B

TAB Key Access

To navigate the User Client Console:

- Press the TAB key to move among the screen elements.
- To load a panel, press the TAB key to the desired link in the navigation pane, then press ENTER. The panel loads into the main pane.
- To display Quick Help, press the TAB key until the focus is on the help icon ?, then press ENTER or the SPACEBAR. To close the Quick Help pane, press ENTER or the SPACEBAR again. Note that Quick Help applies at the panel level; context-sensitive Quick Help is available only when using a mouse.
- To select a check box, press the TAB key to place focus on the box, then press the SPACEBAR. To toggle off the selection, press the SPACEBAR again.
- To activate a button, press the TAB key to place focus on the button, then press ENTER or the SPACEBAR

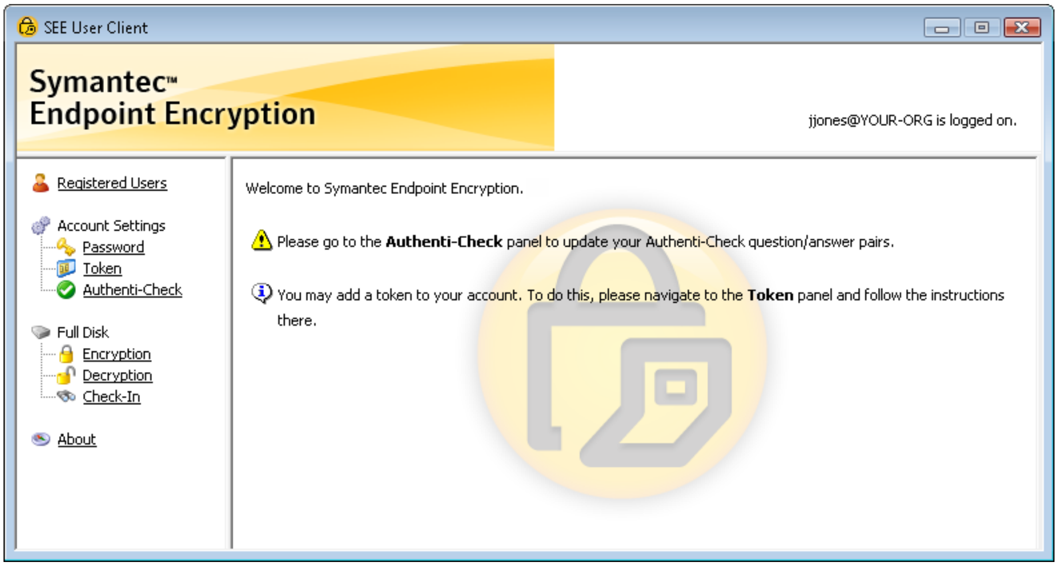
The TAB key follows standard user-interface behavior:

- Tabbing order within each panel is top to bottom, left to right.
- To move forward, press the TAB key; to move backward, press SHIFT+TAB.
- To scroll, use the UP ARROW key and the DOWN ARROW key.

When you use the TAB key to navigate, you may need to press the key more than once to place the focus on the next desired link, input field, button, or icon, depending on the location of the current focus.

Home Panel

The User Client Console opens with the Home panel and an enabled navigation pane.



Welcome to Symantec Endpoint Encryption.

Please go to the **Authenti-Check** panel to update your Authenti-Check question/answer pairs.

You may add a token to your account. To do this, please navigate to the **Token** panel and follow the instructions there.

Figure 5.6—User Client Console Home, with Action Items

From time to time, your Policy Administrator may push out new policies that require you to take action. You will be notified of your action items on the Home panel. If a panel is included in the action item, go to the panel listed by clicking its link, then update the information as specified on the Home panel. Each time you submit the updated information, you are returned to the Home panel and that action item is removed from the list.

Figure 5.6 shows three action items that could appear. All of the possible action items, their meaning, and the action you need to take are described in the following table.

Table 5.2—Home Panel Action Items

Action Item	Meaning	Action
Please go to the Authenti-Check panel to update your Authenti-Check question/answer pairs.	Either the questions and/or their type (pre-defined, required, or optional) have changed, or Authenti-Check is being enabled for the first time.	From the navigation pane, click *Authenti-Check*. Refer to “Authenti-Check Panel” on page 45.
You may add a password to your account. To do this, please navigate to the **Password** panel and follow the instructions there.	You are allowed to authenticate with either a token or a password. You registered with a token but can add a password. Once you have defined both methods, you can use either one to authenticate to Symantec Endpoint Encryption.	From the navigation pane, click *Password*. Refer to “Password Panel” on page 42.

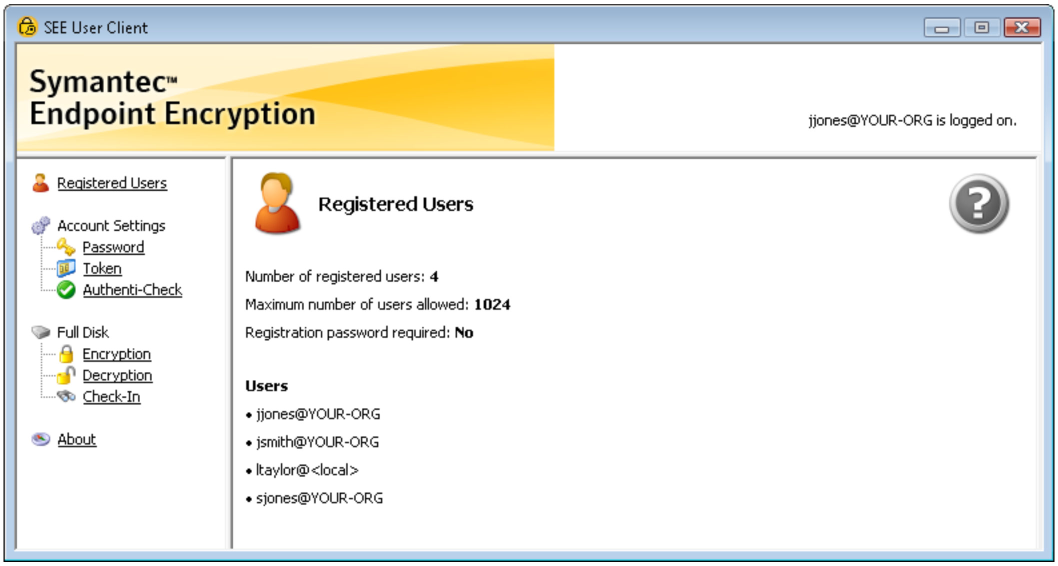
Table 5.2—Home Panel Action Items (Continued)

Action Item	Meaning	Action
You may add a token to your account. To do this, please navigate to the **Token** panel and follow the instructions there.	You are allowed to authenticate with either a token or a password. You registered with a password but can add a token. Once you have defined both methods, you can use either one to authenticate to Symantec Endpoint Encryption.	From the navigation pane, click *Token*. Refer to “Token Panel” on page 44.
Your Symantec Endpoint Encryption password has been changed successfully to match your Windows password.	A Single Sign-On policy has been applied to your account. Full Disk has synchronized your Symantec Endpoint Encryption password with your Windows password.	The next time you log on, use your Windows password as your Symantec Endpoint Encryption password.

Registered Users Panel

The Registered Users panel summarizes policies affecting registered users and lists the users that have registered on this computer.

From the navigation pane click *Registered Users*. The Registered Users panel appears.



Number of registered users: **4**

Maximum number of users allowed: **1024**

Registration password required: **No**

Users

- jjones@YOUR-ORG
- jsmith@YOUR-ORG
- ltaylor@<local>
- sjones@YOUR-ORG

Figure 5.7—User Client Console Registered Users Panel

The top area of the panel provides the maximum number of registered users, the number of users currently registered, and whether or not a registration password is required.

The **Users** area identifies all users registered with Symantec Endpoint Encryption, including yourself. The following table describes the syntax conventions used in this display.

Table 5.3—Registered User Account Display Syntax

Windows User Type	Syntax	Example
Domain	*user name@domain*	jsmith@YOUR-ORG
Local	*user name@*<local>	jsmith@<local>

Password Panel

Basics

You can use the Password panel to change your Symantec Endpoint Encryption password if Single Sign-On is not enabled.

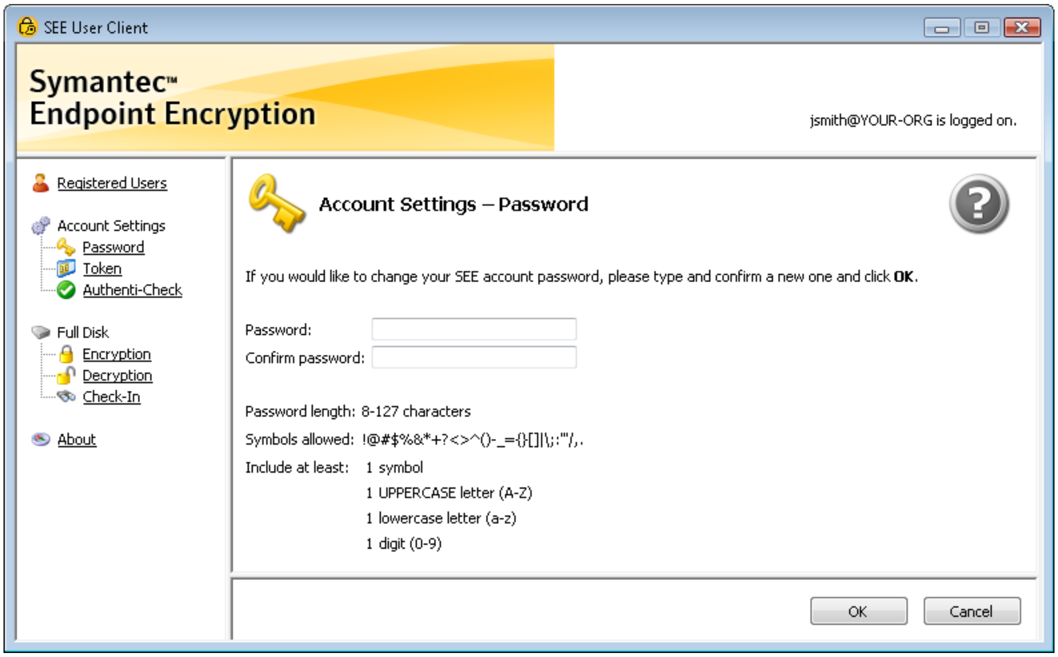
You can also use the Password panel to add a Symantec Endpoint Encryption password if you have your choice of authentication methods: password or token.

If Single Sign-On is enabled, refer to Appendix A “Password Changes with SSO Enabled” on page 55 for password change instructions.

Click *Password* from the navigation pane. The Password panel appears.

Single Sign-On Not Enabled

If Single Sign-On is not enabled and you need to add or change your Symantec Endpoint Encryption password, the **New password** and **Confirm new password** boxes will be displayed.



jsmith@YOUR-ORG is logged on.

If you would like to change your SEE account password, please type and confirm a new one and click **OK**.

Password:

Confirm password:

Password length: 8-127 characters

Symbols allowed: !@#$%&*+?<>^()-_={}[]|\;:'"/,.

Include at least: 1 symbol
1 UPPERCASE letter (A-Z)
1 lowercase letter (a-z)
1 digit (0-9)

Figure 5.8—User Client Console Password Panel, SSO Not Enabled, Existing Password

The text above the **New password** and **Confirm new password** boxes will vary depending on whether or not you have set a Symantec Endpoint Encryption password or not.

In the **New Password** field, type your new Symantec Endpoint Encryption password. In the **Confirm new password** field, type your new password again. For your password to be accepted, it must conform to any requirements shown on the panel for **Password length**, **Symbols allowed**, and **Include at least**.

Only enter characters that can be typed from the keyboard. Using alternate input methods—such as typing from the ALT+numeric keypad—may create characters that you will not be able to enter in the pre-Windows environment.

Click **OK**.

One of the following actions will occur.

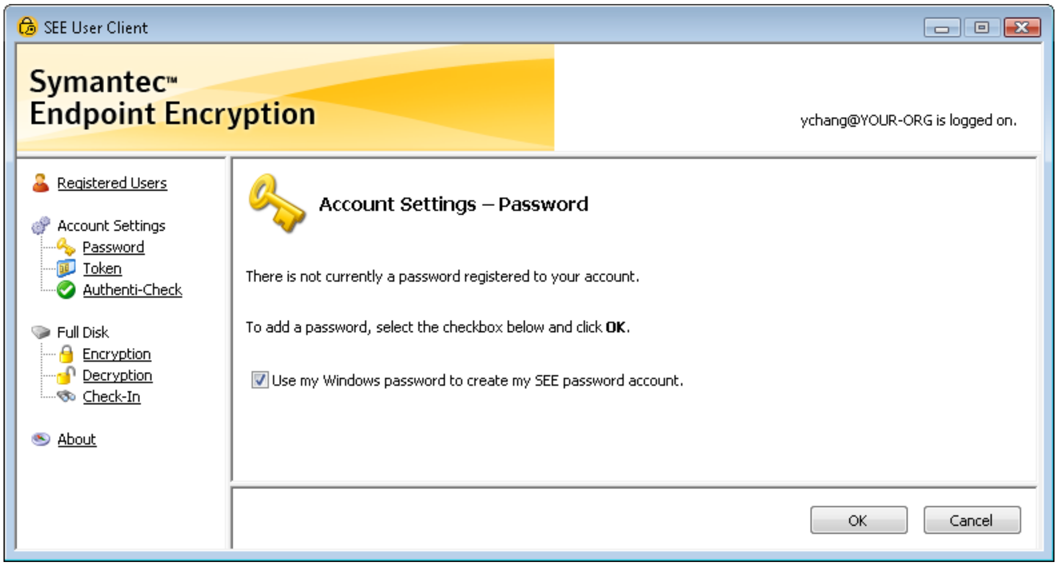
- If your password meets the requirements, your password is updated and the Home panel (“Home Panel” on page 40) replaces the Password panel.
- If the password change is not allowed—for example, if not enough time has elapsed since you last changed your password—the fields and buttons become unavailable. An error message box will inform you of the nature of the problem. On the message box, click **OK** to dismiss the box.
- If the password change is allowed but the password does not comply with the password requirements, then the requirement that the password does not satisfy is highlighted in red. Make the changes necessary to bring it into compliance, then click **OK** to resubmit the password.

At any time you may exit the panel by choosing another task from the navigation pane or clicking the Close button ☒ to quit the User Client Console. Your password will not be changed.

If you click **Cancel**, the fields are cleared and your password is not submitted.

Single Sign-On Enabled

If Single Sign-On is enabled and you have your choice of authentication methods, you can use the Password panel to add a Symantec Endpoint Encryption password to your account. This option is useful if you registered using a token, but have both a token and a password account in Windows, and want to be able to log on to Full Disk with either. To add a password, you must first log on to Windows using your password account. If you aren’t already logged on to Windows with your password account, the Password panel will prompt you to do so.



ychang@YOUR-ORG is logged on.

There is not currently a password registered to your account.

To add a password, select the checkbox below and click **OK**.

☑ Use my Windows password to create my SEE password account.

Figure 5.9—User Client Console Password Panel, SSO Enabled

To add a Symantec Endpoint Encryption password to your account, select the **Use my Windows password to create my Symantec Endpoint Encryption password account** check box. Then click **OK**. A confirmation message will be displayed.

Token Panel

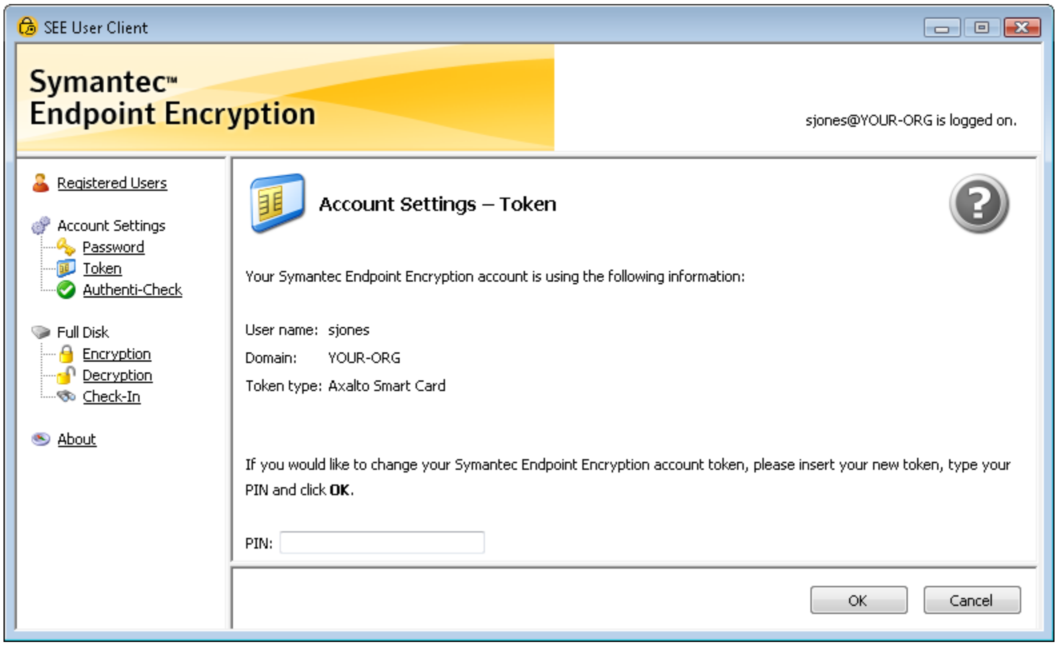
Basics

Use the Token panel to add or change the token that you use to authenticate to Symantec Endpoint Encryption.

From the navigation pane, click *Token*. The Token panel appears.

Token Change

If your administrator has provided you with a new token, you can use the Token panel to associate it with your new account.



Account Settings – Token

Your Symantec Endpoint Encryption account is using the following information:

User name: sjones
Domain: YOUR-ORG
Token type: Axalto Smart Card

If you would like to change your Symantec Endpoint Encryption account token, please insert your new token, type your PIN and click **OK**.

PIN:

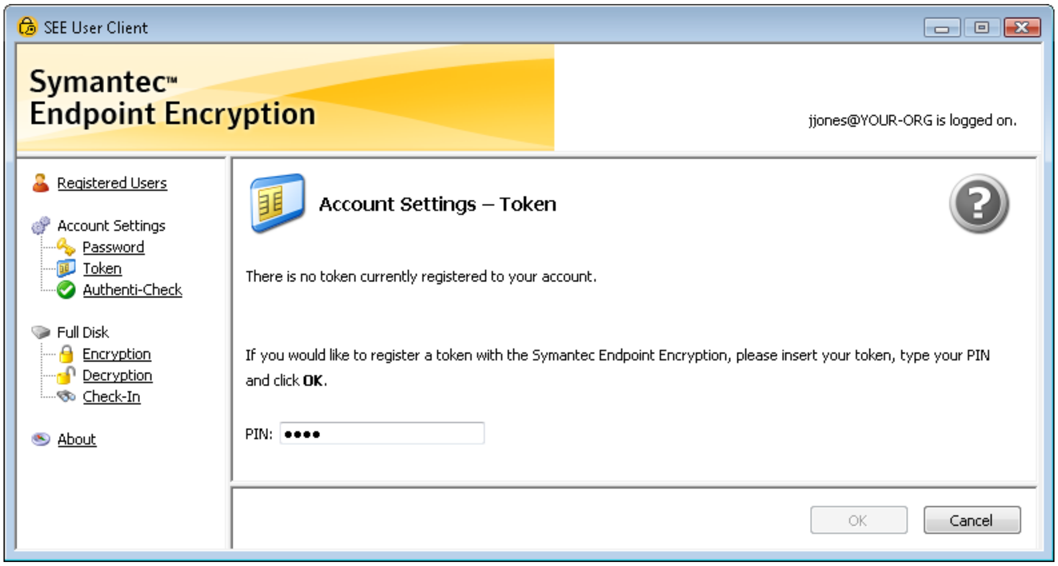
Figure 5.10—User Client Console Token Panel with Existing Token

The top section of the panel will display the token information currently associated with your Symantec Endpoint Encryption account.

To change this token, insert the new token. Type the PIN. Click **OK**.

Token Addition

If you have the option of authenticating with either a password or a token and do not yet have a token associated with your account, the Token panel will provide you with the opportunity of adding one.



Account Settings – Token

There is no token currently registered to your account.

If you would like to register a token with the Symantec Endpoint Encryption, please insert your token, type your PIN and click **OK**.

PIN: ●●●●

Figure 5.11—User Client Console Token Panel without Existing Token

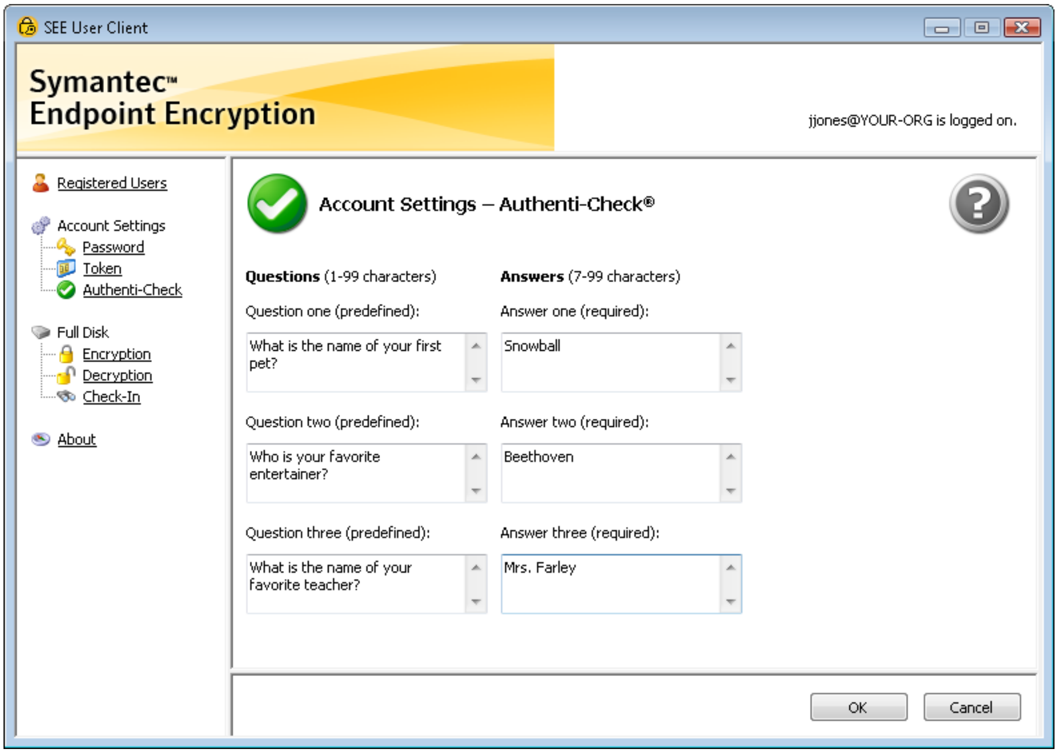
To add a token, insert it. Type the PIN. Click **OK**.

Authenti-Check Panel

Use the Authenti-Check panel to set or modify the question-answer pairs that will allow you to gain access to your computer if you forget your password, token, or PIN.

From the navigation pane, click *Authenti-Check*. The Authenti-Check panel appears.

The following figure shows an example panel with Authenti-Check enabled and three questions predefined. If Authenti-Check is not enabled for you, the main pane will say so. If your computer is set for automatic authentication, this feature will not be available to you.



Symantec™ Endpoint Encryption

jjones@YOUR-ORG is logged on.

Account Settings – Authenti-Check®

Questions (1-99 characters)

Answers (7-99 characters)

Question one (predefined): What is the name of your first pet?

Answer one (required): Snowball

Question two (predefined): Who is your favorite entertainer?

Answer two (required): Beethoven

Question three (predefined): What is the name of your favorite teacher?

Answer three (required): Mrs. Farley

Figure 5.12—User Client Console Authenti-Check Panel

Your Authenti-Check answers will not be displayed, once they have been stored, for security reasons.

Try to choose answers that other people cannot guess easily. Follow similar guidelines for your questions and answers as you would for your password. Create pairs that:

- Do not contain commonly known information,
- Are longer rather than shorter, and
- You can remember without writing down.

The following table provides examples of secure and less secure questions.

Secure	Less Secure
Who was your favorite teacher?	What is your social security number?
Who was your childhood hero?	Where were you born?
What is the street name where your favorite relative lived?	What is your mother’s maiden name?

When entering questions and answers, consider the following:

- Answers are visible when typed, so be sure no one is watching you type them. These answers are as important as your password.

- Remember precisely how you enter the answers; if you must enter them later to recover from a forgotten password, they must match what you enter now. The answers are not case-sensitive.

Questions and answers marked required must be completed. Minimum and maximum character lengths are indicated in parentheses beside **Questions** and **Answers**. Even if a question or answer is marked optional, consider filling it in as it will increase the security of your data.

Only enter characters that can be typed from the keyboard. Using alternate input methods—such as typing from the ALT+numeric keypad—may create characters that you will not be able to enter in the pre-Windows environment.

When you have entered all questions and answers, click **OK** to submit your information.

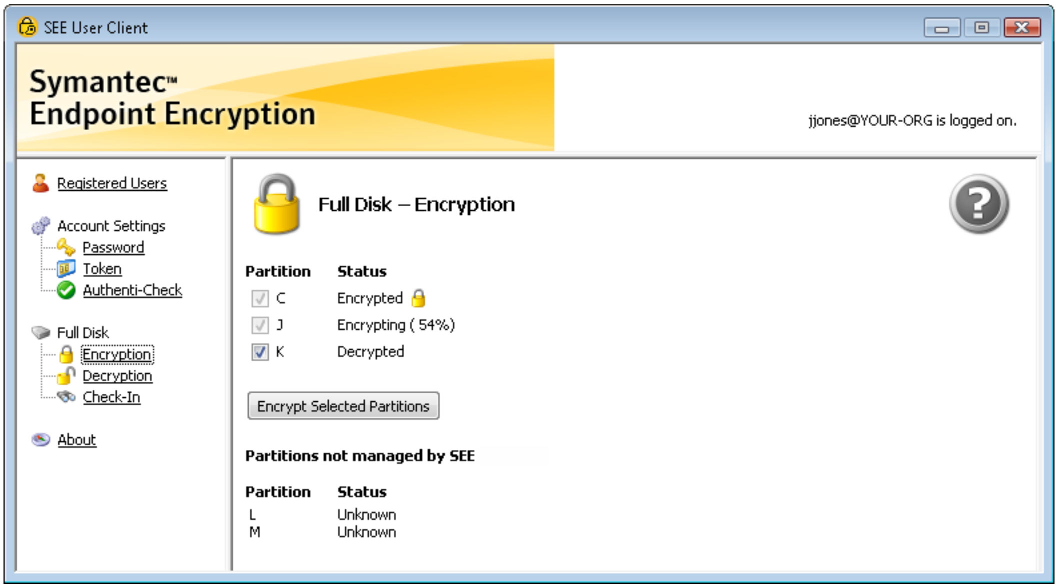
If your questions and answers are accepted, your information is updated. The Home panel (“Home Panel” on page 40) appears, replacing the Authenti-Check panel.

If your questions and answers are not accepted, the field that needs correcting turns red. Make your corrections. Click **OK** again.

If you click **Cancel**, your information is cleared and not submitted.

Encryption Panel

To view the encryption status of your computer or to manually encrypt decrypted partitions, click *Encryption* from the navigation pane. The Encryption panel appears.



Full Disk – Encryption

Partition	Status
☑ C	Encrypted
☑ J	Encrypting (54%)
☑ K	Decrypted

Partitions not managed by SEE

Partition	Status
L	Unknown
M	Unknown

Figure 5.13—User Client Console Encryption Panel

In the **Status** column, one of the following will be displayed for each partition: **Encryption Pending**, **Encrypting**, **Encrypted**, **Decryption Pending**, **Decrypting**, **Decrypted**, or **Unknown**.

The check boxes beside partitions with statuses of **Decryption Pending**, **Decrypting**, and **Decrypted** will be available for selection.

Should you need to encrypt the disk or partition, you should first connect to an uninterruptible power source, since an interruption of power could cause data corruption. For example, if you are encrypting a laptop, plug the laptop in before you start.

Once you select the check box beside one or more partitions, the **Encrypt Selected Partitions** button becomes available. Click **Encrypt Selected Partitions** to begin encrypting the selected partition(s). The partitions will be encrypted one at a time in alphabetical order.

The partition(s) waiting to be encrypted will have a status of **Encryption Pending**. While encryption is running, the panel shows the percentage of encryption, such as **Encrypting (80 %)**. When encryption completes, no percentage is shown; a lock icon 🔒 accompanies the **Encrypted** status for easy visual confirmation that this disk or partition is fully encrypted.

The check boxes beside partitions with statuses of **Encryption Pending**, **Encrypting**, and **Encrypted** will not be available.

You can continue to work normally while partitions are encrypting.

The **Partitions not managed by SEE** area will be displayed if multiple disks exist on the computer and:

- One or more of the additional drives connects through an eSATA port. Full Disk does not manage eSATA drives.
- The primary boot drive is Opal-compliant. Only primary Opal-compliant drives can be managed by Full Disk.
- The **Encrypt boot disk only** option was selected during the creation of the original installation package. The partitions on the additional disk(s) cannot be encrypted or decrypted.

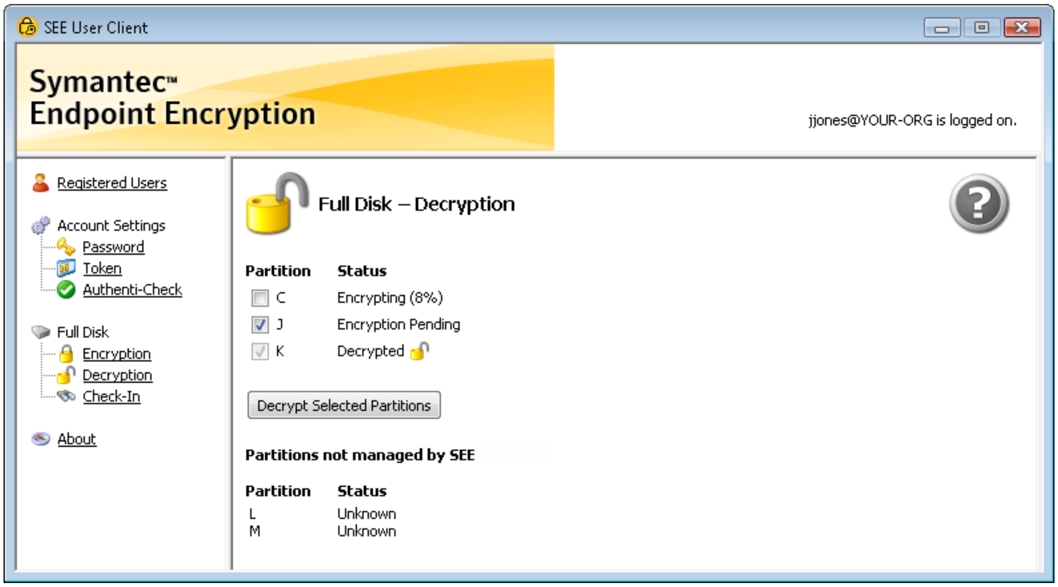
Each partition listed in the **Partitions not managed by SEE** area will have a status of **Unknown**.

Decryption Panel

If you have decryption priviledges and no Opal-compliant drives, you can use the Decryption panel to:

- View drive decryption status
- Decrypt drives

To open the Decryption panel, click *Decryption* from the navigation pane. The Decryption panel appears.



jjones@YOUR-ORG is logged on.

Full Disk – Decryption

Partition	Status
☐ C	Encrypting (8%)
☑ J	Encryption Pending
☑ K	Decrypted 🔓

Decrypt Selected Partitions

Partitions not managed by SEE

Partition	Status
L	Unknown
M	Unknown

Figure 5.14—User Client Console Decryption Panel

Each partition will be listed with one of the following statuses: **Encryption Pending**, **Encrypting**, **Encrypted**, **Decryption Pending**, **Decrypting**, **Decrypted**, or **Unknown**.

Before Full Disk can be uninstalled, all partitions must be decrypted. You must uninstall Full Disk if:

- The operating system is about to be upgraded.
- A major physical change in the core hardware is about to occur. For example, an upgraded processor or motherboard is going to be installed. Changes to the partition table are not possible until Full Disk has been uninstalled.

Should you need to decrypt the disk, first connect to an uninterruptible power source, since an interruption of power could cause data corruption. For example, if you are decrypting a laptop, plug in the laptop before you start.

If a partition is listed with a status of **Encryption Pending**, **Encrypting**, or **Encrypted** you can select the check box beside it. Upon the selection of a check box, the **Decrypt Selected Partitions** button becomes available. Click **Decrypt Selected Partitions** to begin decrypting the selected partition(s). You will be asked to confirm that you really want to decrypt. The partitions will be decrypted one at a time in alphabetical order.

The partition(s) waiting to be decrypted will have a status of **Decryption Pending**. While decryption is running, the panel shows the percentage of partition decryption, such as **Decrypting (20 %)**. When decryption completes, no percentage is shown; an unlock icon 🔓 accompanies the **Decrypted** status for easy visual confirmation that this partition is fully decrypted.

If a partition has a status of **Decryption Pending**, **Decrypting**, or **Decrypted**, its check box will not be available.

You can continue to work normally while partitions are decrypting.

The **Partitions not managed by SEE** area will be displayed if multiple disks exist on the computer and:

- One or more of the additional drives connects through an eSATA port. Full Disk does not manage eSATA drives.
- The primary boot drive is Opal-compliant. Only primary Opal-compliant drives can be managed by Full Disk.
- The **Encrypt boot disk only** option was selected during the creation of the original installation package. The partitions on the additional disk(s) cannot be encrypted or decrypted.

Each partition listed in the **Partitions not managed by SEE** area will have a status of **Unknown**.

Check-In Panel

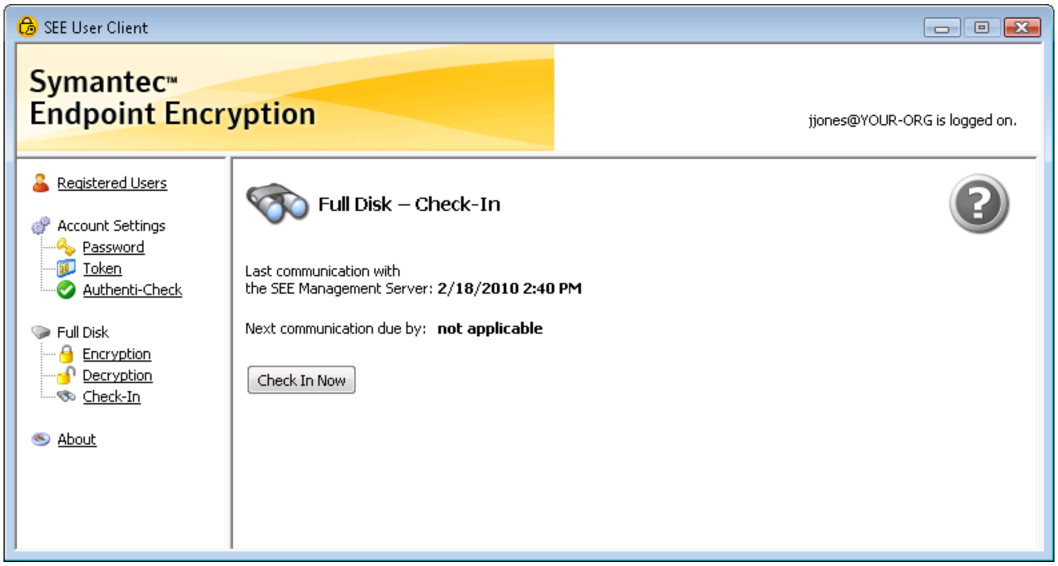
Your computer may have been configured to attempt to connect to the Symantec Endpoint Encryption Management Server at a designated interval. When your computer checks in, it sends information that helps you in the event that you experience difficulty gaining access to Windows.

For security reasons, your Policy Administrator may have set up a check in enforcement. This protects your computer if it gets stolen, by locking out everyone but the Client Administrator after a designated period of time without Symantec Endpoint Encryption Management Server contact.

Use the Check-In panel to:

- See what check-in policy is active.
- Obtain the last communication date information.
- The next communication date information, if check-in is enforced by lockout.
- Force immediate communication with the Symantec Endpoint Encryption Management Server (if enabled by policy).

To access the panel, from the navigation pane click *Check-In*. The Check-In panel appears.



jjones@YOUR-ORG is logged on.

Full Disk – Check-In

Last communication with
the SEE Management Server: **2/18/2010 2:40 PM**

Next communication due by: **not applicable**

Figure 5.15—User Client Console Check-In Panel

Figure 5.15 shows an example of a computer that has checked in and is not subject to a lockout enforcement policy. The information displayed in the Check-In panel is described in the following table.

Table 5.4—Check-In Panel Information

Field Label	Value	Meaning
Last communication with the Symantec Endpoint Encryption Management Server	Date and time	Communication with the Symantec Endpoint Encryption Management Server occurred on the specified date at the specified time.
	never connected	This computer has never connected to the Symantec Endpoint Encryption Management Server.
Next communication due by	Future date and time	A lockout enforcement policy is in effect and your computer must make contact with the Symantec Endpoint Encryption Management Server no later than the specified date and time.
	Past date and time in red with a warning icon ⚠. Tooltip message, “Communication is overdue,” appears.	A lockout enforcement policy is in effect and your computer has failed to connect within the mandatory interval. A lockout is imminent.
	not applicable	A lockout enforcement policy is not in effect.

If the Check-In panel displays the **Check In Now** button, select the button if:

- A lockout enforcement policy is in effect and lockout is imminent.
- You are running a VPN and your computer’s check-in is intermittent.
- Your administrator has asked you to select the button.

After clicking the button, you will see status messages that your computer is attempting to communicate and then whether that attempt was successful. If communication was successful, the **Last communication with the Symantec Endpoint Encryption Management Server** field is updated. If a lockout policy is in effect, the **Next communication due by** field is also updated and any potential lockout is prevented.

If you do not know what has been preventing your computer from checking in with the server, or if you select **Check In Now** and communication fails, contact your Client Administrator. They can extend the **Next communication due by** date if lockout enforcement is in effect, and separately resolve whatever is preventing your computer from making the required contact.

Novell SSO

Basics

If you have Novell Client installed on your computer, the Novell SSO link appears in the navigation pane under Full Disk.

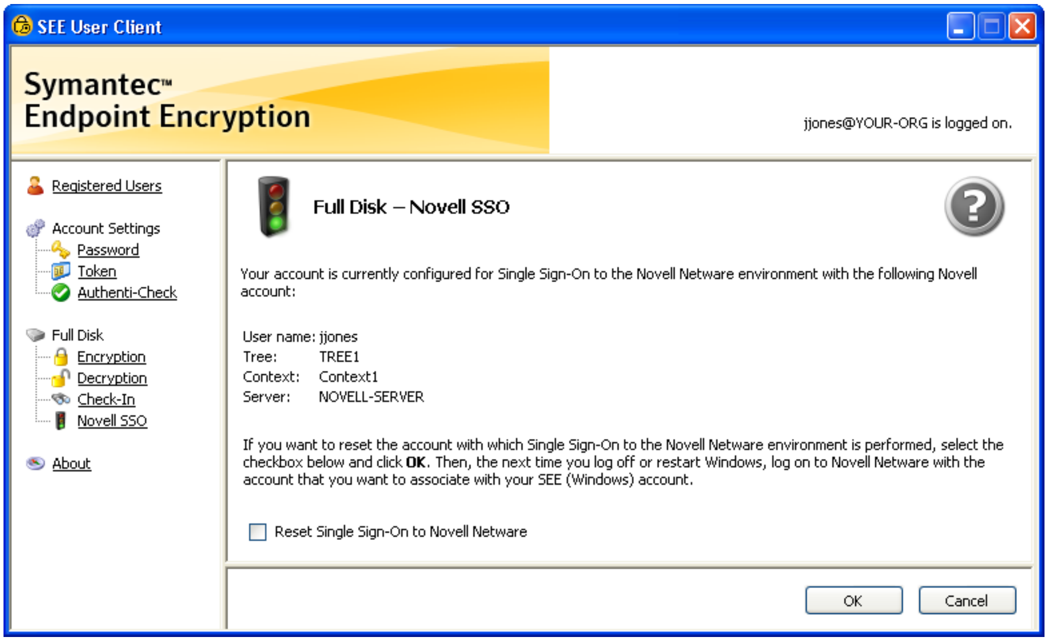
Click *Novell SSO* from the navigation pane, to perform one of the following:

- View the status of your Novell synchronization.
- Reset the Novell account currently configured to be associated with your Windows and Symantec Endpoint Encryption accounts (refer to “Reset Novell SSO” on page 51).
- Configure your Novell account to be associated with your Windows and Symantec Endpoint Encryption accounts (refer to “Turn On Novell SSO” on page 53).

If you click *Novell SSO* and see a message rather than one of the two panels described in this section, contact your Client Administrator.

Reset Novell SSO

If your Novell account has already been set up for Single Sign-On—either during registration or during a prior visit to this panel—the panel will identify the account that you are currently synchronizing with and provide the option to reset your account.



Your account is currently configured for Single Sign-On to the Novell Netware environment with the following Novell account:

User name: jjones
Tree: TREE1
Context: Context1
Server: NOVELL-SERVER

If you want to reset the account with which Single Sign-On to the Novell Netware environment is performed, select the checkbox below and click **OK**. Then, the next time you log off or restart Windows, log on to Novell Netware with the account that you want to associate with your SEE (Windows) account.

□ Reset Single Sign-On to Novell Netware

Figure 5.16—User Client Console Novell SSO Panel, Reset

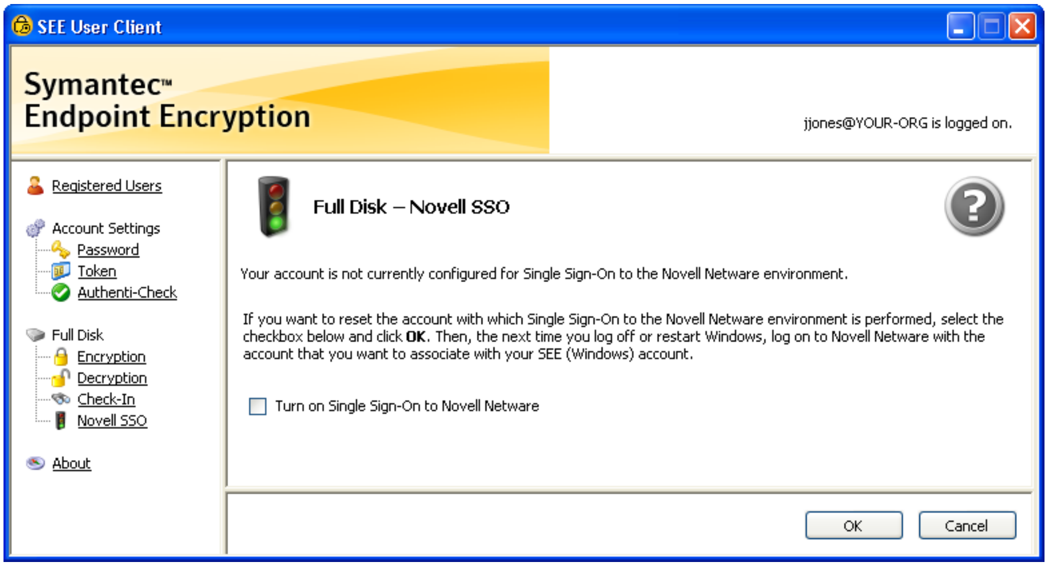
To change the Novell account that you are currently synchronizing with, or if Single Sign-On is not working properly, select the **Reset Single Sign-On to Novell Netware** check box, then click **OK**.

The next time you restart your computer, log on to Novell Netware with the account that you would like to associate with the Windows account that you registered with.

A message will be displayed, confirming the resynchronization.

Turn On Novell SSO

If you have not yet configured your Novell account for Single Sign-On, the panel will state this and offer the option to do so.



jjones@YOUR-ORG is logged on.

Full Disk – Novell SSO

Your account is not currently configured for Single Sign-On to the Novell Netware environment.

If you want to reset the account with which Single Sign-On to the Novell Netware environment is performed, select the checkbox below and click **OK**. Then, the next time you log off or restart Windows, log on to Novell Netware with the account that you want to associate with your SEE (Windows) account.

□ Turn on Single Sign-On to Novell Netware

Figure 5.17—User Client Console Novell SSO Panel, Turn On

If you are a part of a Novell Netware environment, and you would like to log on only once each time you power on your machine, select the **Turn on Single Sign-On to Novell Netware** check box, then click **OK**.

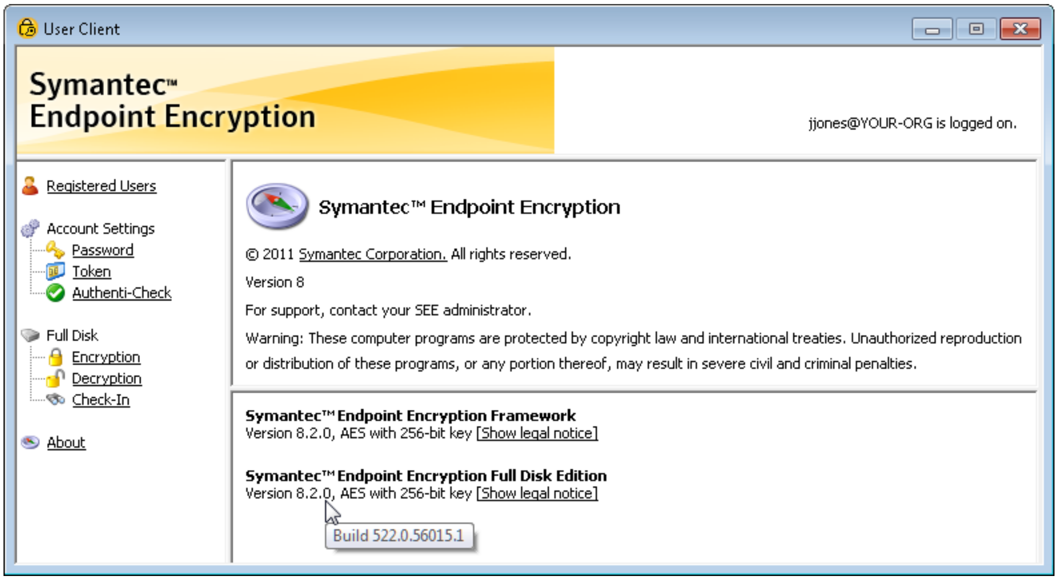
The next time you restart your computer, log on to Novell Netware with the account that you would like to associate with the Windows account that you registered with.

A message will be displayed, confirming the synchronization.

About Panel

Use the About panel to find out which version of Framework and Full Disk you are running.

From the navigation pane, click *About*. The About panel appears.



jjones@YOUR-ORG is logged on.

Symantec™ Endpoint Encryption

© 2011 Symantec Corporation. All rights reserved.

Version 8

For support, contact your SEE administrator.

Warning: These computer programs are protected by copyright law and international treaties. Unauthorized reproduction or distribution of these programs, or any portion thereof, may result in severe civil and criminal penalties.

Symantec™ Endpoint Encryption Framework
Version 8.2.0, AES with 256-bit key [Show legal notice]

Symantec™ Endpoint Encryption Full Disk Edition
Version 8.2.0, AES with 256-bit key [Show legal notice]

Build 522.0.56015.1

Figure 5.18—User Client Console About Panel

The build number is accessible as a Tooltip when you hover your mouse over the version number. The build number can be used to see whether patches have been applied.

From time to time, a service pack number (SP*n*) is appended to the build string, indicating that this is not a major release but an update that fixes existing problems and in some cases delivers product enhancements.

Click *Show legal notice* to see the legal notices associated with a product.

Appendix A. Password Changes with SSO Enabled

Overview

If SSO is enabled, follow the instructions in this Appendix to achieve a change in your password.

Procedure for Expired Password

Your administrator may have set a policy that requires you to change your password after a set period of time. For example, you may be forced to change your password every three months.

Windows will prompt you to change your password each time you log on. Before proceeding to change your password, power the machine off and then back on. Complete pre-boot authentication. Then go ahead and change your password as prompted.

Procedure for Compromised Password

You may want to change your password even though you aren’t required to. You may believe that your password has been compromised, for example.

To change your password, complete the following steps:

1. Go to the machine that you registered on.
2. Power the machine on.
3. Complete pre-boot authentication.
4. Once Windows has loaded, press CTRL+ALT+DEL.
5. Click **Change Password** or **Change a Password**, as per your version of Windows.
6. Provide your old password and your new password.

Appendix B. Token Usage & Error Messages

Overview

This appendix describes correct token insertion, and token behavior when information is being read from your token.

It also lists the error and warning messages that you may encounter while using a token to:

- Register for a Symantec Endpoint Encryption account or re-register for an account when required to change your authentication method.
- Authenticate in pre-Windows.
- Authenticate to the User Client Console.

In some cases, the message itself contains the default instruction: *Please call the help desk for assistance.* This instruction appears in the Message column in italics. The instruction is configurable by your administrator, so your instruction may differ from the default shown in these tables.

Token Usage

Insertion

To insert your token, follow the instruction for the appropriate token type:

- *Smart card*—hold the card so that the side containing the gold chip is on top and the card end containing the chip is closest to the reader.
- *USB-based*—connect the USB-connector end of your token to a USB port or into a USB extension cable attached to your computer.

Recognition

Make sure that the token software recognizes your token before you remove it, by referring to the appropriate description below:

- *Aladdin eToken*—the red light on the token itself blinks while the token is being read; the icon in the Windows notification area does not change.
- *Common Access Card (CAC) and Personal Identity Verification (PIV)*—the icon in your Windows notification area shows just a reader when the token is not inserted, then adds a blue token when the token has been inserted and read.
- *RSA token*—the icon in the Windows notification area changes to include a plus sign.
- *SafeSign v2.1*—no visual sign appears in the Windows notification area; simply wait a few moments after token insertion.
- *Smart card*—the icon's computer screen changes from black to blue while the icon's golden token blinks, then returns to black when the blinking stops.

If your token or the reader has a light, it blinks when information from your token is being read. Wait until all blinking stops before taking the next action, such as clicking **Log On**. Do not remove the token until token reading is complete.

If you encounter token or certificate errors, refer to the next section for possible causes and resolution.

Error Messages

Registration/Re-Registration

Table B.1 lists the error messages that may occur when you are initially registering for your Symantec Endpoint Encryption account, or when you are re-registering in response to a policy change or upgrade that requires you to change your account authentication method.

Table B.1—Registration Messages

Token Type	Message	Meaning	Action
All	Incorrect PIN.	You entered an incorrect PIN.	Carefully re-enter your PIN; if you enter an incorrect PIN too many times, your PIN could become blocked. Click **Next**.
All	The PIN is blocked for this token. The token needs to be replaced or modified by an administrator. *Please call the help desk for assistance.*	The number of remaining attempts on your token is zero.	Follow the instructions for getting assistance. Your PIN is blocked.
All	The token has been removed. Please reinsert the token.	You removed the token before the registration process completed.	Reinsert the token and leave it inserted until you click **Finish** on the final registration panel.
All	A certificate validation error has occurred. The token needs to be replaced or modified by an administrator. *Please call the help desk for assistance.*	Your token does not contain any certificate, or your token contains an invalid certificate.	Follow the instructions for getting assistance. Your token does not contain a valid certificate.
All	The certificate selection failed. The token may need to be replaced or modified by an administrator. *Please call the help desk for assistance.*	The certificate could not be retrieved from the local certificate store.	Follow the instructions for getting assistance. The certificate(s) on your token may be invalid or your token software is not configured add your certificate(s) to the local Windows certificate store each time you insert your token.

Table B.1—Registration Messages (Continued)

Token Type	Message	Meaning	Action
All	A token error has occurred. The registration process cannot continue. *Please call the help desk for assistance.*	The token is unknown or the reader is not supported.	Check that you have inserted the token issued to you for Symantec Endpoint Encryption use. If you used the incorrect token, insert the correct token, and try again. If you continue to receive this message, follow the instructions for getting assistance. The type of token you are using may not be the type of token selected by your Policy Administrator during product installation, or the token or the token reader may not be supported by Symantec Endpoint Encryption.
All	The program could not verify your credentials.	The verification process failed.	Contact the appropriate administrator. You cannot authenticate.

Pre-Windows Logon

Table B.2 lists the error messages that may be generated when you attempt to log on to Full Disk in pre-Windows.

Table B.2—Pre-Windows Logon Messages

Token Type	Message	Meaning	Action
CAC / Smart Card	The inserted token is not responding. Please make sure the token is inserted correctly and try again.	Your token is not inserted correctly.	Refer to “Token Usage” on page 56 for detailed information about proper token insertion. Remove the token. Reinsert the token in the appropriate manner. Click **OK** on the message.
CAC / Smart Card	The inserted token could not be recognized. You will need to use a token that can be recognized by the system.	The type of token you are attempting to log on with does not match the type of token your administrator configured for your use.	Remove the incorrect token, then insert the correct one. If you do not know which token or card type is correct—or you have not been issued the correct card—contact the appropriate administrator

Table B.2—Pre-Windows Logon Messages (Continued)

Token Type	Message	Meaning	Action
Smart Card	A matching certificate could not be found on this token. The current token will need to be replaced or modified by an administrator. Please try to use Logon Assistance from the Password Logon screen.	No registered user account that matches the certificate(s) on your token could be found. You may have the wrong token, a new token, or your token may not have any certificates on it at all.	Click **OK**. Remove your token. You will be returned to the Startup screen. Press CTRL+ALT+DEL. The **Logon** for password users will be displayed. Type your user name, select your domain, and click **Logon Assistance**.
All	An error has occurred. The machine needs to be restarted.	Something unexpected happened during communication between the token and the reader.	Click **Restart Computer** from the message box. Confirm that you are using the correct token and that your reader is supported. Reinsert the token in the reader and try again. If this message reappears, contact your Client Administrator.
All	A certificate validation error has occurred. The current token will need to be replaced or modified by an administrator. *Please call the help desk for assistance.*	The certificate on this token is not within its period of validity. Your certificate was issued today, but is not yet valid because the Certificate Authority issues certificates using Greenwich Mean Time (GMT). Therefore, your local system date has not yet caught up with the GMT activation date.	Either wait for the local system time to catch up with GMT or contact the person who issued this token to you.
All	Incorrect PIN.	You inserted your token for the Startup screen but did not enter your PIN—or you entered an incorrect PIN—on the Logon screen before clicking **OK**.	Check your PIN, then type your PIN and click **OK.** Take care as you type your PIN, since submitting the wrong PIN a number of times could result in a blocked PIN. If you do not remember your PIN, click **Logon Assistance** and refer to Chapter 4 “Logon Assistance Request” on page 22. If you do not have logon assistance features available, contact your Client Administrator.

Table B.2—Pre-Windows Logon Messages (Continued)

Token Type	Message	Meaning	Action
All	Symantec Endpoint Encryption Full Disk has detected that the token has been removed. Please click OK to restart the login process.	You removed your token before your logon process was complete.	Reinsert your token. The Startup screen will be displayed. Insert your token or your token and token reader. The Logon for tokens will be displayed. Type your PIN then click **OK**.
		Your token reader was unplugged after Full Disk detected your token.	Plug the reader back in, then reboot. Insert your token at the Startup screen to bring up the Logon screen. Type your PIN then click **OK**.
All	The PIN is blocked for this token. The current token needs to be replaced or modified by an administrator. *Please call the help desk for assistance.*	Your PIN has been blocked by your token software for exceeding the maximum number of incorrect retries to enter your PIN.	Follow the instructions for getting assistance. Your PIN is blocked and the token needs to be replaced or modified.

User Client Console Logon

Table B.3 lists the error messages that may occur when you are trying to log on to the User Client Console using a token.

Table B.3—User Client Console Logon Messages

Token Type	Message	Meaning	Action
All	Incorrect PIN.	You entered an incorrect PIN.	Check your PIN, then type your PIN again and click **Log On.** Take care as you type your PIN, since resubmitting the wrong PIN a number of times could result in a blocked PIN. If you are not sure of your PIN, contact the administrator who manages your token.
All	The PIN is blocked for this token. The token needs to be replaced or modified by an administrator. *Please call the help desk for assistance.*	The number of remaining attempts on your token is zero.	Follow the instructions in the error message for getting assistance. Your PIN is blocked and your token needs to be replaced or modified.
All	The program could not log you on. The token was removed.	You removed the token immediately after clicking **Log On**.	Reinsert the token and leave it inserted until you are logged on to the User Client Console.

Table B.3—User Client Console Logon Messages (Continued)

Token Type	Message	Meaning	Action
All	A token error has occurred. The authentication process cannot continue. *Please call the help desk for assistance.*	The token is unknown or the reader is not supported.	Follow the instructions in the error message for getting assistance.
All	A certificate validation error has occurred. The token needs to be replaced or modified by an administrator. *Please call the help desk for assistance.*	Your token does not contain any certificate, your token contains an invalid certificate, or your PIN has expired.	Follow the instructions in the error message for getting assistance.
All	The certificate selection failed. The token may need to be replaced or modified by an administrator. *Please call the help desk for assistance.*	The certificate could not be retrieved from the local certificate store.	Follow the instructions for getting assistance. The certificate(s) on your token may be invalid or your token software is not configured add your certificate(s) to the local Windows certificate store each time you insert your token.
All	The program could not log you on. Your credentials could not be verified.	The authentication process failed.	Make sure the inserted token is the one that you registered for your Symantec Endpoint Encryption account. If it is not, remove the invalid token and insert the valid token. Try to log on again. If you continue to receive this message, contact the administrator who manages your token.

Appendix C. Logon Audio Cues

Overview

Should you be visually impaired or experiencing trouble with your monitor, Full Disk provides audio cues through your computer's internal speaker to escort you through the pre-Windows logon process.

Enablement

1. If you are a token user, ensure that your token is not inserted.
2. Power the computer on.
3. Wait approximately one minute. This allows the Startup screen to load.
4. Press F5.
5. One long beep sounds, indicating that audio cues are enabled. This beep is immediately followed by a short beep, indicating the presence of the Startup screen.
6. If you heard the beeps, proceed to the next section. If not, contact your Client Administrator.

Usage

Basics

Each time you restart your computer, after approximately one minute a short beep sounds, indicating the presence of the Startup screen.

If you hear five beeps instead of a short beep, call your Client Administrator. Your computer is in a lockout or pre-lockout condition.

Go to the appropriate section for a description of the sequence of audio beeps that sound during the pre-Windows authentication process:

- If you are a password-based user, continue to the next section.
- If you are a token-based user, skip to "Token Logon" on page 63.

Password Logon

Logon Window

1. After powering on the computer and hearing the short beep that indicates the presence of the Startup screen, press CTRL+ALT+DEL to launch the Logon window.
2. Two beeps sound, indicating that the cursor is in the **User name** field. Type your user name.
3. Press TAB.
4. Three beeps sound, indicating that the cursor is in the **Password** field. Type your password.
5. Press ENTER.

One of three possible beep sequences will sound. Table C.1 lists the possibilities.

Table C.1—Possible Responses to Password Credential Submittal

Audio Beeps	Meaning	Next Action
1 beep	Successful logon	You have completed the pre-Windows logon sequence. If Single Sign-On is not enabled, you will be at the Windows prompt. If Single Sign-On is enabled, you will be admitted to Windows.
4 beeps	Incorrect logon	Press ENTER to dismiss the incorrect logon message. Return to Step 2 in this section to try again.
6 more beeps, following the 4 beeps	Logon delay	Reference “Logon Delay” on page 63.

Logon Delay

If you provide incorrect logon information too many times, you may be forced to wait before you can try to log on again. This forced delay prevents unauthorized users from breaking in to your system with automated guessing tools.

If six beeps sound following the four beeps that indicated an incorrect logon, wait. The logon delay screen is active.

When the logon delay completes, two beeps sound. Return to Step 2 in this section and try again.

While the logon delay screen is active, do not click your mouse. The focus is on the **Logon Assistance** button. If you click this button, you will be taken into the logon assistance wizard.

Token Logon

1. Before powering on the computer, remove your token. After powering on the computer and hearing the short beep that indicates the presence of the Startup screen, insert your token to launch the Logon window.
2. Three beeps sound, indicating that the cursor is in the **PIN** field. Type your PIN.
3. Press ENTER. Do not remove your token until processing completes.

Two possible beep sequences will sound. Table C.2 lists the possibilities.

Table C.2—Possible Responses to Token Credential Submittal

Audio Beeps	Meaning	Next Action
1 beep	Successful logon	You have completed the pre-Windows logon sequence. If Single Sign-On is not enabled, you will be at the Windows prompt. If Single Sign-On is enabled, you will be admitted to Windows.
4 beeps	Incorrect logon	Press ENTER to dismiss the incorrect PIN message. Return to Step 2 in this section to try again. Note that your token software may be configured to block your PIN after too many incorrect attempts, so be sure you know your PIN before retrying.

Cancelling the Logon Process

To cancel the logon process, from the Logon screen press ESC. One short beep sounds, indicating the presence of the Startup screen.

Turning Off Audio Cues

Press F5 from the Startup screen. The audio cues are toggled off.

Glossary

Administrator Client Console

Provides Client Administrators with features for encrypting or decrypting the computer’s hard disk, extending a check-in date, and unregistering user accounts.

Authentication Method

Specifies how registered users and Client Administrators authenticate to Symantec Endpoint Encryption. Methods include password, token, password and token, or automatic. If Single Sign-On is enabled, the authentication method used for Symantec Endpoint Encryption and Windows must be the same method. If the Policy Administrator changes the authentication method, registered users may be forced to re-register.

Authenti-Check

Allows users on Windows endpoints to recover from forgotten credentials without help desk assistance. The user authenticates with a set of up to three question-answer pairs. Authenti-Check is not available to Client Administrators or Mac users.

Autologon

Allows Policy Administrators to remotely deploy software to computers protected by Full Disk. Software installations typically require several restarts, and Autologon allows pre-boot authentication to be bypassed, so that the computer does not require any credentials before loading Windows.

Automatic Authentication

If a Client Computer is set for automatic authentication, Full Disk will not require a user to provide Symantec Endpoint Encryption credentials before allowing Windows to load. This option relies on Windows to authenticate users.

In addition, users will be registered automatically unless a registration password is required. Requiring a registration password serves to avoid reaching the maximum registered user limit and to limit the number of users that can gain access to the User Client Console. If a user is re-registering, a registration password is not required.

The automatic authentication feature is not available for Mac endpoints.

Client Administrator

Provides local support to Symantec Endpoint Encryption users. The Policy Administrator assigns each Client Administrator account individual administrative privileges:

- *Unregister users*—allows Client Administrators to unregister registered users;
- *Decrypt drives*—provides Client Administrators with the right to decrypt drives encrypted by Symantec Endpoint Encryption Full Disk;
- *Extend lockout*—permits Client Administrators to extend the Client Computer’s next communication date; and
- *Unlock*—enables Client Administrators to unlock Client Computers that have been locked for failure to communicate with the Symantec Endpoint Encryption Management Server.

Client Administrators are always able to authenticate to Client Computers.

Client Administrators cannot change their own passwords or use any password-recovery methods.

Client Database

The client database consists of a series of volume files and is part of the Symantec Endpoint Encryption file system. Once the location of the client database files has been specified during the creation of the Client Computer installation packages and the installation has completed, these files must never be moved or disturbed.

Grace Restarts

A grace restart allows Windows to load without requiring the first user to register.

Lockout

A lockout occurs if a computer fails to check in with the Symantec Endpoint Encryption Management Server within the prescribed interval. Users cannot gain access to Windows. Only a Client Administrator can log on. A user may be able to regain access to the computer by using the One-Time Password (OTP) feature with help desk assistance.

One-Time Password (OTP) Program

The One-Time Password (OTP) Program allows Full Disk users on Windows endpoints to recover from a forgotten password, PIN, or token with help desk assistance. Users can also use the OTP program to regain access to their Windows computer after it has been locked for a failure to communicate with the Symantec Endpoint Encryption Management Server. To complete the OTP process the user must contact the help desk.

Policy Administrator

Performs centralized administration of Symantec Endpoint Encryption. Using the Manager Console and the Manager Computer, the Policy Administrator:

- Updates and sets client policies.
- Issues commands to encrypt or decrypt drives on fixed disks that are not Opal-compliant
- Runs reports.
- Changes the Management Password.
- Runs the Help Desk Program.
- Creates the computer-specific Recover DAT file necessary for Recover /B, for Recover /O, and Recover /S.

Domain or higher-level administrators can restrict access to Symantec Endpoint Encryption snap-ins when assigning specific Policy Administrator duties.

Pre-Windows Environment

The Pre-Windows environment loads upon reboot, before the Windows operating system. This environment helps protect the Client Computer’s hard disks by requiring authentication before a user gains access to Windows.

Registration

During registration, users set their credentials so that they can authenticate in pre-Windows. In addition, users may be asked to set password recovery information. Registration may be configured to occur with or without the user’s intervention. The first user is required to register after the designated number of grace restarts has expired.

Re-Registration

Symantec Endpoint Encryption users may be required to re-register if a Policy Administrator issues a computer policy or installs an upgrade package that requires them to change their authentication method.

Single Sign-On (SSO)

If SSO is enabled, the user logs on once in pre-Windows and is then authenticated to Windows.

Symantec Endpoint Encryption Framework

Provides Symantec Endpoint Encryption–wide features, such as authentication methods and settings, as well as registered user and Client Administrator accounts and information.

Symantec Endpoint Encryption Password

Used by users and Client Administrators for Pre-Windows authentication and Client Console logons.

Also used by Client Administrators to authenticate to Recover /A and Recover /D.

Unregistration

The removal of a Symantec Endpoint Encryption registered user account, either manually by a Client Administrator or automatically by policy.

User

At least one user must register with Symantec Endpoint Encryption on each Client Computer. A wizard guides the user through the registration process, which involves a maximum of five screens. The registration process can also be configured to occur without user intervention.

Users authenticate to Full Disk in one of three ways:

- *Single Sign-On enabled*—The user is prompted to authenticate each time they restart their computer.
- *Single Sign-On not enabled*—The user must log on twice: once to Full Disk and then separately to Windows.
- *Automatic authentication enabled*—The user is not prompted for Full Disk credentials; the authentication process is transparent. This option relies on Windows to validate the user's credentials.

On Mac endpoints, the first user account is created at the time that encryption of the disk is manually initiated. Additional user accounts can be added later.

Index