Table of contents

Data Privacy and Protection: The Need to Encrypt ........................................... Page 3
Logging into Endpoint Encryption for the first time ................................... Page 4
Local Recovery – Enrolment ......................................................................... Page 5
Regular logons with Endpoint Encryption .............................................. Page 6
Performing a Local Recovery ....................................................................... Page 7
Performing a User Recovery ......................................................................... Page 8
MEE Windows Client Interface ................................................................... Page 10
Software not to use ...................................................................................... Page 11
Getting assistance ....................................................................................... Page 11
Data Privacy and Protection: The Need to Encrypt

Section 36 of the Newfoundland and Labrador Access to Information and Protection of Privacy Act requires public bodies "...protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal." In keeping with rulings in other jurisdictions, the provincial privacy commissioner has ruled that encryption "[is] the required industry standard with respect to technological safeguards." ¹

In order to ensure compliance with provincial ATIPP legislation as well as internal privacy policy, Memorial University is updating its electronic data security policy. A cornerstone of these revisions will be full disk encryption of laptops containing sensitive University information. After careful evaluation, McAfee Endpoint Encryption was chosen to be the University's new full disk encryption standard.

Logging into Endpoint Encryption for the first time

When you first login to McAfee Endpoint Encryption you will be prompted to set a new password and also be prompted to answer four security questions. These questions can later be used to reset your password if you cannot remember it.

After turning on your laptop, you will see the following screen:

**Login Process**

1.) Type your assigned username and password. Click Ok.
2.) You will be asked to change your password. It must meet the following complexity requirements:
   a. At least one letter (a-z,A-Z)
   b. At least one digit (0-9)
   c. At least one symbol ( !@#$%^&*+-.....)
   d. Passwords must be a minimum of 8 characters in length
3.) Click finish.
4.) Local enrolment. Select Ok to set up Local Recovery Questions or cancel to proceed with windows logon.
Local Recovery – Enrolment

After successfully setting your password, you will be prompted to answer four security questions which can later be used to do a Local Recovery. If you choose not to set up your Local Recovery questions immediately you can cancel and continue the login process. Please note, you will be prompted to set up your Local Recovery questions each time you log in. You can ignore enrolment for up to 10 login attempts. After 10 logins you will no longer be able to bypass enrolment and you will have to set up your Local Recovery Questions. If / when you have to do a Local Recovery, you must type the answers to these security questions exactly as you answer them here.

Please note that the enrolment process allows you to choose from a list of questions. You are not limited solely to the one presented to you. We encourage clients to review the questions and select those which are most relevant and which are likely to be remembered should they need to avail of Local Recovery.
Regular Logons with Endpoint Encryption

After your first time logon, subsequent logons will require your username and the password you created. After turning on your laptop, you will see the following screen:

Login Process

1.) Type your assigned username and password. Click Ok.
2.) Windows will boot as normal.
Performing a Local Recovery

Local recovery is self recovery. Users will not require Service Desk assistance to reset a forgotten MEE password if they can correctly answer the four (4) challenge response questions they set up at some time during their first 10 login attempts.

Warning: Excessive login attempts will invalidate your password only token. Should this happen you will have to contact the Service Desk to recover your password. If your login has failed more than five times we recommend you contact the Service Desk or attempt User Recovery as follows:

Clear the login prompt from your screen by clicking cancel or the x in the upper right hand corner of the screen. On the lower left hand side of the screen you will see a red icon next to the word Options. Clicking on either the icon or the word will expose a menu with three possible selections. Choose “Recovery” to display the Recovery Window. MEE is now in Recovery Mode. Choose “Local Recovery” from the list of options by selecting the appropriate radio button. Upon selecting Local recovery the User Name textbox will become active. Enter your user id in the textbox and click “Next.” The user will then be asked to successfully answer four (4) challenge response questions. Click “next” to proceed to the next question.

If you are successful in answering the questions presented you will be notified that your password is now the default and must be changed. At this point you will enter and confirm a new MEE password. The password change dialog will disappear and the user will have to click on “Password Only Token” to bring up the login screen. Users can then login with their user name and the password they just created.
Performing a User Recovery – Service Desk Assisted

User Recovery is Service Desk assisted password recovery. Users will be required to contact the Service Desk (737-4595) in order to speak with an agent and have their password reset.

**Warning:** Excessive login attempts will invalidate your password only token. Should this happen you will have to contact the Service Desk to recover your password. If your login has failed more than five times, and you cannot avail of the challenge response based Local Recovery we recommend you contact the Service Desk and attempt User Recovery as follows:

Clear the login prompt from your screen by clicking cancel or the x in the upper right hand corner of the screen. On the lower left had side of the screen you will see a red icon next to the word Options. Clicking on either the icon or the word will expose a menu with three possible selections. Choose “Recovery” to display the Recovery Window. MEE is now in Recovery Mode. Choose “User Recovery” from the list of options by selecting the appropriate radio button. Upon selecting User Recovery the User Name textbox will become active. Enter your user id in the textbox and click “Next”.

Contact the Service Desk (737-4595) and advise the agent that you need to perform a User Recovery for MEE. After confirming your identity the agent will login to a web console that will allow him or her to work with you through the process. When prompted provide the Service Desk agent with the sixteen
(16) digit Client code. Please note that a phonetic version of the Client Code is viewable on the screen and may assist you with communicating the code. Once the Client Code is entered and verified by the Service Desk Agent click “Next” to proceed.

The resulting screen allows the entry of a seventeen (17) character code that is communicated by the Service Desk Agent and must be entered by the client. Once the code is entered, click “Finish” to complete the process.

This process will cause the client password to revert to the default value allowing the client to authenticate and reset their MEE password.
MEE Windows Client Interface

When receiving assistance from the Service Desk a user may be asked to perform certain tasks on the laptop through MEE’s windows client. This section will show you the client interface. The client appears as an icon in the bottom right section of the task bar. Right Clicking on the icon will bring up a menu.

The setting you will most likely need in this menu is the “Show Status” option. Clicking on this will bring up the client status monitor. You may be asked to read log data or click the synchronize button to force a sync with the MEE server.
Software not to use

Do not use any third-party defrag or disk recovery tools; doing so may cause data loss. It is safe to use the defrag utility native to Windows. If you are unsure, call the Service Desk to ask if the software is compatible with McAfee Endpoint Encryption.

Getting assistance

If you receive a message saying that your token has been invalidated, you will need to contact the Service Desk to do a password recovery.

If you require assistance for any issues you have McAfee Endpoint Encryption, please call the Service Desk at 737-4595, or email help@mun.ca