

ATA-3 Proposal
Security Mode
Pete McLean - Maxtor
(303) 678-2149
pete_mclean@maxtor.com

The following additions are proposed. Locations and format are based on the current ATA-2 document.

7.5 Security Mode Feature Set

The Security Mode Feature Set provides a method for limiting access to data stored on small form factor hard disk drives to only authorized users or host systems. To accomplish this, a drive is placed in "secure mode" by a user. Having done so, whenever the drive is placed in a host, it must be "unlocked" before it will execute data transfer commands. "Unlocking" is accomplished by providing the drive with a valid "password".

Whether a drive supports secure mode and, if so, the secure mode state can be determined by issuing a SECURE STATE command.

The drive may be set into either Secure Mode Read Only where the drive may be read but not written, or Secure Mode Read/Write where no data transfers can be executed.

The drive is set into "secure mode" by a SET SECURE RO or SET SECURE RW command. The user may set up to four "passwords" each up to 512 bytes in length and the host system will create an "emergency password". The user may also specify that one or more of the "passwords" must be matched to "unlock" the drive. The number of matches required to unlock the drive is placed in the Features register before issuing the SET SECURE XX command. The SET SECURE XX command resembles a write command in that the sector count is valid and the command includes the transfer of n sectors of data to the drive. Each of the n sectors represents a unique "password". If the user defined password contains fewer than 512 bytes, the password will be zero filled to complete a full sector, so that a password sent when the drive is installed on one system will be exactly the same as a password sent when installed on another system.

When in "secure mode" and "locked", non-data transfer commands will be executed normally, however, all data transfer commands, i.e., commands that read or modify user data on the disk, will be rejected with error if in Secure Mode RW and write commands, i.e., commands that modify user data on the disk, will be rejected if in Secure Mode RO. When "unlocked", all commands will execute normally.

The DISABLE SECURE command will allow the drive to be taken out of "secure mode". If in "secure mode" and "unlocked", a drive will accept the DISABLE SECURE command and go out of "secure mode" and delete all passwords. If the drive is in "secure mode" and has not been "unlocked", it will reject the command with errors set.

When inserted/powered up, the drive will go through the standard startup and the state of "secure mode" will be noted. If in "Secure Mode RW" and "locked", the drive will respond to non-data transfer commands but will reject transfer commands until an UNLOCK command is received. If in "Secure Mode RO" and "locked, the drive will reject all write commands until an UNLOCK command is received. The UNLOCK command again resembles a write command. It must have sector count set at the number of sector matches required to unlock the drive and will include the transfer of one sector of data to the memory card for each required match. When data is received, it will not be written, instead it will be compared to the valid "passwords" stored. If the required matches are found, the drive will "unlock" and function normally. If no match is found, errors will be reported in response to the command and the drive

will remain "locked". An unlock command with only one password, the emergency password will always unlock the drive.

When the drive is unlocked, a flag tells the drive when to relock. It may be set such that the drive will automatically lock when powered down or it may require a LOCK command to lock the drive. The flag to disable locking at power down is provided for systems that frequently remove power from the drive. The passwords remain valid, and normal secure mode locking at power down can be re-enabled by issuing another UNLOCK command.

When the UNLOCK command is issued and the drive is already in the unlocked state, the command is executed and if the match count and passwords are not valid, i.e., the command would not have unlocked the drive an error is returned. Thus when in unlocked state, passwords can be verified using the UNLOCK command. The flag for locking the drive at power down must be valid when verifying passwords.

The LOCK command locks the drive immediately on receipt.

The ADD PASSWORDS, REMOVE PASSWORDS, and MODIFY MATCH commands allow the user to modify the set of passwords and number of matches required to unlock the drive.

The following entries are added to Table 9, Clause 7.4 Status and Error Posting.

	Status Register				Error Register					
	DRDY	DF	CORR	ERR	BBK	UNC	IDNF	ABRT	TK0NF	AMNF
SECURE STATE	V	V		V				V		
SET SECURE RW	V	V		V				V		
SET SECURE RO	V	V		V				V		
ADD PASSWORDS	V	V		V				V		
REMOVE PASSWORDS	V	V		V				V		
MODIFY MATCH	V	V		V				V		
DISABLE SECURE	V	V		V				V		
UNLOCK	V	V		V				V		
LOCK	V	V		V				V		

The following entries are added to Table 10, Clause 8. Command Descriptions.

proto		typ	Command code	Parameters Used				
				FR	SC	SN	CY	DH
ND	SECURE STATE	O	EAh	y		80h	y	D
PO	SET SECURE RW	O	EBh	y	y	81h	y	D
PO	SET SECURE RO	O	EBh	y	y	82h	y	D
PO	ADD PASSWORDS	O	EBh	y	y	83h	y	D
PO	REMOVE PASSWORDS	O	EBh	y	y	84h	y	D
ND	MODIFY MATCH	O	EAh	y		85h	y	D
ND	DISABLE SECURE	O	EAh			86h	y	D
PO	UNLOCK	O	EBh	y	y	87h	y	D
ND	LOCK	O	EAh			88h	y	D

The following commands descriptions are added to Clause 8. Command Descriptions.

SECURE STATE

TYPE - Optional - Security Mode Feature Set.

PROTOCOL - Non-data command.

INPUTS - The Sector Number register is set to 80h. The Cylinder High register is set to 53h (ascii "S"). The Cylinder Low register is set to 4Dh (ascii "M").

NORMAL OUTPUTS - The Cylinder High register is set to ACh. The Cylinder Low register is set to B2h. The Features register is set to the version number of the Secure Mode Feature Set implemented by the device, 01h. The Sector Count register contains the Security Mode state as shown in table S1.

7	6	5	4	3	2	1	0
Secure Set R/W	Secure Set RO	Unlocked	Lock Flag	r	Match Count		

Table S1 - Security Mode state

Bit 7 - Secure Set R/W - If set, indicates the device has been set in Secure Mode Read/Write.

Bit 6 - Secure Set RO - If set, indicates the device has been set in Secure Mode Read Only.

Bit 5 - Unlocked - If set, indicates the device has been unlocked.

Bit 4 - Lock Flag - If the device is in Secure Mode and this bit is cleared, the device will assume the locked state when powered down. If the device is in Secure Mode and this bit is set, the device can only be locked by issuing a Lock command.

Bit 3 - reserved

Bit 2:0 - Value indicates the number of password matches required to unlock the device.

ERROR OUTPUTS - Aborted Command error if the device does not support the Secure Mode Feature Set. Aborted Command error if the device supports the Secure Mode Feature Set and the values in the Cylinder High or Cylinder Low registers were incorrect.

PREREQUISITES - None.

DESCRIPTION - This command returns the Secure Mode state of a device that implements the Secure Mode Function Set. Upon completion of the command, the Sector Count register contains the Secure Mode state as shown if table S1. The contents of the Cylinder High and Cylinder Low registers will be ACh and B2h respectively. The Features register will contain the version number of the Secure Mode version implemented by the device, 01h for this version of this standard.

SET SECURE RW

TYPE - Optional - Security Mode Feature Set.

PROTOCOL - PIO data out.

INPUTS - The Sector Number register is set to 81h. The Sector Count register is set to the number of passwords to be set including the Emergency password. Bits 6 through 0 of the Features register are set to indicate the number of password matches to be required to Unlock the device. If Bit 7 of the Features register is set, the first password received is considered the Emergency password. The Cylinder High register is set to 53h (ascii "S"). The Cylinder Low register is set to 4Dh (ascii "M").

NORMAL OUTPUTS - The Cylinder High register is set to ACh. The Cylinder Low register is set to B2h.

ERROR OUTPUTS - Aborted Command error if:

- the device does not support the Secure Mode Feature Set.

- the device supports the Secure Mode Feature Set and the values in the Cylinder High or Cylinder Low registers are incorrect.

- the device supports the Secure Mode Feature Set and the device is already in Secure Mode.

- the device supports the Secure Mode Feature Set and the number of passwords indicated in the Sector Count register is less than one or greater than five.

- the device supports the Secure Mode Feature Set and the number of matches indicated in the Features register is less than one or greater than the number of passwords set in the Sector Count register.

PREREQUISITES - The device must not be in Secure Mode.

DESCRIPTION - This command is used to set a drive into Secure Mode Read/Write, define the valid set of passwords and the number of password matches required to unlock a drive.

If the drive is not in Secure Mode when the command is received, the value set in the Features register indicates the number of matches that will be required to unlock the drive. The value set in the Sector Count register indicates the number of 512 byte passwords that will be passed with this command including the Emergency password. If either the Features register low order four bits or the Sector Count register contain a value less than 1 or greater than 5, the command is not executed and Abort error is returned. If the number in the Features register low order four bits is greater than the number in the Sector Count register, the command is not executed and Abort error is returned.

Use of the Emergency password is optional. If the most significant bit of the Features register is set, the first password received by the drive is considered to be the Emergency password. The number of matches required and the passwords received with the command become the valid passwords and match count values. Upon successful completion of this command, the secure state will reflect Secure Mode RW set, unlocked, value 101. The contents of the Cylinder Registers will be ACh and B2h.

The Emergency password shall be created by the host by asking the user a series of questions. This password will consist of 18 twenty byte fields. Each field will contain the ASCII response to one question. If the user response is longer than twenty bytes, the field will contain the first twenty bytes of the response (i.e., response will be truncated). If the response is less than twenty bytes the end of the field will be zero filled. The last 152 bytes of the password will be zero filled. The Emergency password may only be modified by removing the drive from secure mode, then setting into secure mode again. The questions in order are shown in table S2.

Question	Field	Password bytes
Last Name?	0	0-19
First Name?	1	20-39
Home address - street?	2	40-59
Home address - city?	3	60-79
Home address - state?	4	80-99
Home Address - country?	5	100-119
Home phone number?	6	120-139
Employer's name?	7	140-159
Work address - street?	8	160-179
Work address - city?	9	180-199
Work address - state?	10	200-219
Work address - country?	11	220-239
Work phone number?	12	240-259
Place of birth - city?	13	260-279
Place of birth - state?	14	280-299
Place of birth - country?	15	300-319
Date of birth?	16	320-339
Mother's maiden name?	17	340-359
Zero fill		360-511

Table S2 - Emergency Password Questions

If the drive is in Secure Mode when this command is received, the command will not be executed and an Abort error is returned.

SET SECURE RO

TYPE - Optional - Security Mode Feature Set.

PROTOCOL - PIO data out.

INPUTS - The Sector Number register is set to 82h. The Sector Count register is set to the number of passwords to be set including the Emergency password. Bits 6 through 0 of the Features register are set to indicate the number of password matches to be required to Unlock the device. If Bit 7 of the Features register is set, the first password received is considered the Emergency password. The Cylinder High register is set to 53h (ascii "S"). The Cylinder Low register is set to 4Dh (ascii "M").

NORMAL OUTPUTS - The Cylinder High register is set to ACh. The Cylinder Low register is set to B2h.

ERROR OUTPUTS - Aborted Command error if:

- the device does not support the Secure Mode Feature Set.

- the device supports the Secure Mode Feature Set and the values in the Cylinder High or Cylinder Low registers are incorrect.

- the device supports the Secure Mode Feature Set and the device is already in Secure Mode.

- the device supports the Secure Mode Feature Set and the number of passwords indicated in the Sector Count register is less than one or greater than five.

- the device supports the Secure Mode Feature Set and the number of matches indicated in the Features register is less than one or greater than the number of passwords set in the Sector Count register.

PREREQUISITES - The device must not be in Secure Mode.

DESCRIPTION - This command is used to set a drive into Secure Mode Read Only, define the valid set of passwords and the number of password matches required to unlock a drive.

If the drive is not in Secure Mode when the command is received, the value set in the Features register indicates the number of matches that will be required to unlock the drive. The value set in the Sector Count register indicates the number of 512 byte passwords that will be passed with this command including the Emergency password. If either the Features register low order four bits or the Sector Count register contain a value less than 1 or greater than 5, the command is not executed and Abort error is returned. If the number in the Features register low order four bits is greater than the number in the Sector Count register, the command is not executed and Abort error is returned.

Use of the Emergency password is optional. If the most significant bit of the Features register is set, the first password received by the drive is considered to be the Emergency password. The number of matches required and the passwords received with the command become the valid passwords and match count values. Upon successful completion of this command, the secure state will reflect Secure Mode RO set, unlocked, value 101. The contents of the Cylinder Registers will be ACh and B2h.

The Emergency password shall be created by the host by asking the user a series of questions. This password will consist of 18 twenty byte fields. Each field will contain the ASCII response to one question. If the user response is longer than twenty bytes, the field will contain the first twenty bytes of the response (i.e., response will be truncated). If the response is less than twenty bytes the end of the field will be zero filled. The last 152 bytes of the password will be zero filled. The Emergency password may only be modified by removing the drive from secure mode, then setting into secure mode again. The questions in order are shown in table S3.

Question	Field	Password bytes
Last Name?	0	0-19
First Name?	1	20-39
Home address - street?	2	40-59
Home address - city?	3	60-79
Home address - state?	4	80-99
Home Address - country?	5	100-119
Home phone number?	6	120-139
Employer's name?	7	140-159
Work address - street?	8	160-179
Work address - city?	9	180-199
Work address - state?	10	200-219
Work address - country?	11	220-239
Work phone number?	12	240-259
Place of birth - city?	13	260-279
Place of birth - state?	14	280-299
Place of birth - country?	15	300-319
Date of birth?	16	320-339
Mother's maiden name?	17	340-359
Zero fill		360-511

Table S3 - Emergency Password Questions

If the drive is in Secure Mode when this command is received, the command will not be executed and an Abort error is returned.

ADD PASSWORD

TYPE - Optional - Security Mode Feature Set.

PROTOCOL - PIO data out.

INPUTS - The Sector Number register is set to 83h. The Sector Count register is set to the number of passwords to be added to the existing set of passwords. Bits 6 through 0 of the Features register are set to indicate the number of password matches to be required to Unlock the device. Bit 7 of the Features register shall be 0. The Cylinder High register is set to 53h (ascii "S"). The Cylinder Low register is set to 4Dh (ascii "M").

NORMAL OUTPUTS - The Cylinder High register is set to ACh. The Cylinder Low register is set to B2h.

ERROR OUTPUTS - Aborted Command error if:

- the device does not support the Secure Mode Feature Set.

- the device supports the Secure Mode Feature Set and the values in the Cylinder High or Cylinder Low registers are incorrect.

- the device supports the Secure Mode Feature Set and the device is not already in Secure Mode.

- the device supports the Secure Mode Feature Set, is in Secure Mode and Locked.

- the device supports the Secure Mode Feature Set and the number of passwords indicated in the Sector Count register plus the number of passwords already set is less than one or greater than five.

- the device supports the Secure Mode Feature Set and the number of matches indicated in the Features register is less than one or greater than the number of passwords set in the Sector Count register plus the number of passwords already set.

PREREQUISITES - The device must be in Secure Mode and Unlocked.

DESCRIPTION - When the drive is in Secure Mode XX and Unlocked, with an existing match count and set of valid passwords, this command is used to add passwords to the existing set of valid passwords and reset the match count.

The value in the Features register will become the new match count value. The value in the Sector Count register indicates the number of passwords to be added. If the value in the Sector Count register is zero, or if the value in the Sector Count register plus the existing number of valid passwords is greater than 5, the command will be rejected and an Abort error returned. If the value in the Features register is less than 1 or greater than the value in the Sector Count register plus the number of existing valid passwords, the command will be rejected and an Abort error returned.

Upon successful completion of this command, the passwords received with this command will be added to the set of existing passwords, the match count value will be the new match count value, and the drive will be in Secure Mode XX, unlocked state.

If this command is received when not in Secure Mode XX, unlocked state, the command will be rejected and an Abort error returned.

REMOVE PASSWORD

TYPE - Optional - Security Mode Feature Set.

PROTOCOL - PIO data out.

INPUTS - The Sector Number register is set to 84h. The Sector Count register is set to the number of passwords to be removed from the existing set of passwords. Bits 6 through 0 of the Features register are set to indicate the number of password matches to be required to Unlock the device. Bit 7 of the Features register shall be 0. The Cylinder High register is set to 53h (ascii "S"). The Cylinder Low register is set to 4Dh (ascii "M").

NORMAL OUTPUTS - The Cylinder High register is set to ACh. The Cylinder Low register is set to B2h.

ERROR OUTPUTS - Aborted Command error if:

- the device does not support the Secure Mode Feature Set.

- the device supports the Secure Mode Feature Set and the values in the Cylinder High or Cylinder Low registers are incorrect.

- the device supports the Secure Mode Feature Set and the device is not already in Secure Mode.

- the device supports the Secure Mode Feature Set, is in Secure Mode and Locked.

- the device supports the Secure Mode Feature Set and the number of passwords already set minus the number of passwords indicated in the Sector Count register is less than one.

- the device supports the Secure Mode Feature Set and the number of matches indicated in the Features register is less than one or greater than the number of passwords already set minus the number of passwords set in the Sector Count register.

PREREQUISITES - The device must be in Secure Mode and Unlocked.

DESCRIPTION - When the drive is in Secure Mode XX, unlocked, with an existing match count and set of valid passwords, this command is used to remove passwords from the existing set of valid passwords and reset the match count.

The value in the Features register will become the new match count value. The value in the Sector Count register indicates the number of passwords to be removed. If the existing number of valid passwords minus the value in the Sector Count register is less than 1, the command will be rejected and an Abort error returned. If the value in the Features register is less than 1 or greater than the number of existing valid passwords minus the value in the Sector Count register, the command will be rejected and an Abort error returned. The emergency password may not be removed and the command will be rejected with an Abort error if this is attempted.

Upon successful completion of this command, the passwords received with this command will be compared with the set of existing passwords and each that matches with a different password will be removed from the valid set of passwords. Passwords that do not match any valid passwords do not affect the set of valid passwords. The match count value will be the new match count value, and the drive will be in Secure Mode XX, unlocked state.

If this command is received when not in Secure Mode XX, unlocked state, the command will be rejected and an Abort error returned.

MODIFY MATCH

TYPE - Optional - Security Mode Feature Set.

PROTOCOL - Non-data command.

INPUTS - The Sector Number register is set to 85h. Bits 6 through 0 of the Features register are set to indicate the number of password matches to be required to Unlock the device. Bit 7 of the Features register shall be 0. The Cylinder High register is set to 53h (ascii "S"). The Cylinder Low register is set to 4Dh (ascii "M").

NORMAL OUTPUTS - The Cylinder High register is set to ACh. The Cylinder Low register is set to B2h.

ERROR OUTPUTS - Aborted Command error if:

- the device does not support the Secure Mode Feature Set.

- the device supports the Secure Mode Feature Set and the values in the Cylinder High or Cylinder Low registers are incorrect.

- the device supports the Secure Mode Feature Set and the device is not already in Secure Mode.

- the device supports the Secure Mode Feature Set, is in Secure Mode and Locked.

- the device supports the Secure Mode Feature Set and the number of matches indicated in the Features register is less than one or greater than the number of passwords already set.

PREREQUISITES - The device must be in Secure Mode and Unlocked.

DESCRIPTION - When the drive is in Secure Mode XX, unlocked, with an existing match count and set of valid passwords, this command is used to reset only the match count.

The value in the Features register will become the new match count value. If the value in the Features register is less than 1 or greater than the number of existing valid passwords, the command will be rejected and an Abort error returned.

Upon successful completion of this command, the match count value will be the new match count value, and the drive will be in Secure Mode XX, unlocked state.

If this command is received when not in Secure Mode XX, unlocked state, the command will be rejected and an Abort error returned.

DISABLE SECURE

TYPE - Optional - Security Mode Feature Set.

PROTOCOL - Non-data command.

INPUTS - The Sector Number register is set to 86h. The Cylinder High register is set to 53h (ascii "S"). The Cylinder Low register is set to 4Dh (ascii "M").

NORMAL OUTPUTS - The Cylinder High register is set to ACh. The Cylinder Low register is set to B2h.

ERROR OUTPUTS - Aborted Command error if:

- the device does not support the Secure Mode Feature Set.

- the device supports the Secure Mode Feature Set and the values in the Cylinder High or Cylinder Low registers are incorrect.

- the device supports the Secure Mode Feature Set and the device is not already in Secure Mode.

- the device supports the Secure Mode Feature Set, is in Secure Mode and Locked.

PREREQUISITES - The device must be in Secure Mode and Unlocked.

DESCRIPTION - When the drive is in Secure Mode XX, unlocked, with an existing match count and set of valid passwords, this command is used to remove the drive from Secure Mode.

Upon successful completion of this command, the drive will not be in Secure Mode. All passwords are deleted.

If this command is received when not in Secure Mode XX, unlocked state, the command will be rejected and an Abort error returned.

UNLOCK

TYPE - Optional - Security Mode Feature Set.

PROTOCOL - PIO data out.

INPUTS - The Sector Number register is set to 87h. The Sector Count register is set to the number of passwords to be matched. The Features register is set to 00h or Ffh. The Cylinder High register is set to 53h (ascii "S"). The Cylinder Low register is set to 4Dh (ascii "M").

NORMAL OUTPUTS - The Cylinder High register is set to ACh. The Cylinder Low register is set to B2h.

ERROR OUTPUTS - Aborted Command error if:

- the device does not support the Secure Mode Feature Set.

- the device supports the Secure Mode Feature Set and the values in the Cylinder High or Cylinder Low registers are incorrect.

- the device supports the Secure Mode Feature Set and the device is not already in Secure Mode.

- the device supports the Secure Mode Feature Set and the number of passwords indicated in the Sector Count register is not equal to the number of password matches set.

PREREQUISITES - The device must be in Secure Mode.

DESCRIPTION - This command unlocks a drive in the Secure Mode, locked state to allow data transfers.

If the user has forgotten the user defined passwords, the host may recreate the emergency password by asking the questions described in the SET_SECURE_XX command.

If the sector count register contains the value 1 and the password received is the emergency password the command will execute and the drive will unlock. Otherwise, the sector count register will contain the number of 512 byte passwords to be passed to the drive and matched. If this number is not equal to the number of matches specified when the drive was placed in Secure Mode, the command will be rejected and the Abort error returned.

The drive will match the password(s) received with this command with the existing set of valid passwords. If each unlock password matches with a different password in the established set of passwords, the drive will unlock.

For example, if the number of matches is specified as one and the set of passwords consists of four passwords, the single password received with the UNLOCK command will be compared to each of the four possibilities until a match is found.

If the number of matches is specified as two and the set of passwords consists of three passwords, the first password received with the UNLOCK command will be compared to each of the three possibilities until a match is found, and then the second password received with the UNLOCK command will be compared to the remaining two possibilities until a match is found.

If the UNLOCK was successful, the Features register indicates the required action to relock the drive. If the Features register contains the value 00h, the drive will assume the lock state when powered-down. If the Features register contains the value FFh, the drive will only assume the locked state when the LOCK command is received, that is, the drive may be powered-down and back up without assuming the locked state. Passwords remain valid.

If the value in the Features register is other than 00h or FFh, or if the required number of passwords received with the command do not match existing valid passwords, the command is rejected, an Abort error is returned, and the drive will remain in secure mode XX set, locked state. If eight UNLOCK commands are rejected with error, the drive will cease response to any command until powered-down and re powered-up.

If this command is received when the drive is in Secure Mode XX, unlocked state, the command will be executed and if the match count or passwords do not match, an Abort error will be returned but the drive will remain unlocked. Thus when in the unlocked state, this command can be used to verify match count and passwords. The Features register is used as described above to set or clear the Lock Flag.

Upon successful completion, the secure state will reflect Secure Mode XX set and unlocked. Having been unlocked, the drive will now accept and execute all data transfer commands.

If this command is received when not in Secure Mode, the command will be rejected and an Abort error returned.

LOCK

TYPE - Optional - Security Mode Feature Set.

PROTOCOL - Non-data command.

INPUTS - The Sector Number register is set to 88h. The Cylinder High register is set to 53h (ascii "S"). The Cylinder Low register is set to 4Dh (ascii "M").

NORMAL OUTPUTS - The Cylinder High register is set to ACh. The Cylinder Low register is set to B2h.

ERROR OUTPUTS - Aborted Command error if:

- the device does not support the Secure Mode Feature Set.

- the device supports the Secure Mode Feature Set and the values in the Cylinder High or Cylinder Low registers are incorrect.

- the device supports the Secure Mode Feature Set and the device is not already in Secure Mode.

- the device supports the Secure Mode Feature Set, is in Secure Mode and Locked.

PREREQUISITES - The device must be in Secure Mode and Unlocked.

DESCRIPTION - This command will lock a drive any time the drive is in secure mode XX, unlocked. If the drive was unlocked with the Features register value FFh, this is the only means of locking the drive. If the drive was unlocked with the Features register value 00h, either this command or powering-down the drive will cause the drive to assume the locked state.

Upon successful completion of this command the drive will be in secure mode XX, locked, state.

If this command is received when the drive is not in Secure Mode, or in Secure Mode XX, locked, state, the command will be rejected and an Abort error returned.