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 data access to only authorized users or host systems. To accomplish this, an extent on the device is placed in "secure mode" by a user. Having done so, whenever the device is placed in a host, the extent must be "unlocked" before data transfer commands can be executed to it. "Unlocking" is accomplished by providing the device with a valid "password".

Alternatively, a device may be placed in a write protected mode so that data cannot be accidentially overwritten.

Whether a device supports secure mode can be determined by executing an IDENTIFY DEVICE command. The secure mode state can be determined by issuing a SECURE STATE command.

The extent on the device may be set into either Secure Mode Read Only where the extent may be read but not written, or Secure Mode Read/Write where no data transfers can be executed. Or, the device may be set into Secure Mode Write Protect where writes are prevented but the device may be removed from this mode withotu the use of a password.

The extent is set into "secure mode" by a SECURE ENABLE RO or SECURE ENABLE RW command. The user may set up to the maximum number of passwords supported by the device, each password up to 512 bytes in length and the host system will create an "emergency password". The SECURE ENABLE 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 device. 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 device is installed on one system will be exactly the same as a password sent when installed on another system.

The starting address of the extent to be placed in “secure mode” is also included in the SECURE ENABLE XX command. The extent placed in secure mode will then consist of all addresses from that address to the last sector on the device inclusive. If the starting address provided is address zero, the entire device will be placed into secure mode. In this way, a user may protect the data on the entire device or may choose to allow access or booting from one portion of the device and protect data only on the extent specified.

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

A device is placed into Secure Mode WP by simply issuing a SECURE ENABLE WP command.

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

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

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

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

The SECURE LOCK command locks the extent immediately on receipt.

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 DISABLE	V	V		V				V		
SECURE ENABLE RO	V	V		V				V		
SECURE ENABLE RW	V	V		V				V		
SECURE ENABLE WP	V	V		V				V		
SECURE LOCK	V	V		V				V		
SECURE STATE	V	V		V				V		
SECURE UNLOCK	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 DISABLE	O	EAh	y				D
PO	SECURE ENABLE RO	O	EBh	y	y	y	y	y
PO	SECURE ENABLE RW	O	EBh	y	y	y	y	y
ND	SECURE ENABLE WP	O	EAh	y				D
ND	SECURE LOCK	O	EAh	y				D
ND	SECURE STATE	O	EAh	y	y			D
PO	SECURE UNLOCK	O	EBh	y	y			D

The following field definitions are added to the IDENTIFY DEVICE response, clause 8.10.

Word	F/V	
?	F	15 1 = Security Mode Feature Set Supported 14-8 Maximum number of passwords supported 7-0 Version number, 03h for this specification

Word ?: Security Mode Feature Set Support

Bit 15 of word ? is used to indicate the device supports the Secure Mode Feature Set. The field, bits 14-8, indicate the maximum number of passwords the device can support including the Emergency password. The field, bits 7-0, indicate the version of the Secure Mode Feature Set supported, 03h for this specification.

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

SECURE DISABLE

OPCODE - EAh

TYPE - Optional - Security Mode Feature Set.

PROTOCOL - Non-data command.

INPUTS - The Feature register shall be set to 80h.

NORMAL OUTPUTS - none.

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 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 device has an extent that is in Secure Mode RO or RW, unlocked, with an existing set of valid passwords, this command shall remove that extent from Secure Mode. When the device is in Secure Mode WP, this command shall remove the device from Secure Mode.

Upon successful completion of this command, the device shall not be in Secure Mode. All passwords shall be deleted.

If this command is received when not in Secure Mode RO or RW and unlocked state, or Secure Mode WP, the command shall be rejected and an Abort error returned.

SECURE ENABLE RO

OPCODE - EBh

TYPE - Optional - Security Mode Feature Set.

PROTOCOL - PIO data out.

INPUTS - The Features register shall be set to 81h. The Sector Count register specifies the number of passwords to be set including the Emergency password. The Sector Number, Device/Head, Cylinder Low, and Cylinder High registers specify the starting address, either C-H-S or LBA as applicable, of the extent to be placed in Security mode.

NORMAL OUTPUTS - none.

ERROR OUTPUTS - Aborted Command error if:

the device does not support the Secure Mode Feature Set.
the device has already had a Secure Mode extent defined.
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 that supported by the device.
the address indicated is greater than the maximum address supported by the device.

PREREQUISITES - The device must not be in Secure Mode.

DESCRIPTION - This command shall set an extent on the device into Secure Mode Read Only and define the valid set of passwords.

If the device is not in Secure Mode when the command is received, 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 the Sector Count register contains a value less than 1 or greater than the maximum number of passwords supported by the device, the command shall not be executed and Abort error shall be returned.

The address contained in the Sector Number, Device/Head, Cylinder Low and Cylinder High registers indicates the starting address of the extent to be placed in Secure Mode. This extent includes all addresses from this address to the maximum address on the device inclusive. If this address is all zeros, the entire device shall be placed into Secure Mode.

Use of the Emergency password is optional. Upon successful completion of this command, the secure state shall reflect Secure Mode RO set, unlocked.

The Emergency password shall be created by the host by asking the user a single of question, what is your mother’s maiden name. The Emergency password shall consist of the user’s response as an ASCII byte stream followed by zero fill to the 512 byte password size.

If an extent of the device is in Secure Mode when this command is received, the command shall not be executed and an Abort error shall be returned.

SECURE ENABLE RW

OPCODE - EBh

TYPE - Optional - Security Mode Feature Set.

PROTOCOL - PIO data out.

INPUTS - The Features register shall be set to 82h. The Sector Count register specifies the number of passwords to be set including the Emergency password. The Sector Number, Device/Head, Cylinder Low, and Cylinder High registers specify the starting address, either C-H-S or LBA as applicable, of the extent to be placed in Security mode.

NORMAL OUTPUTS - none.

ERROR OUTPUTS - Aborted Command error if:

the device does not support the Secure Mode Feature Set.
the device has already had a Secure Mode extent defined.
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 that supported by the device.
the address indicated is greater than the maximum address supported by the device.

PREREQUISITES - The device must not be in Secure Mode.

DESCRIPTION - This command shall set an extent on the device into Secure Mode Read/Write and define the valid set of passwords.

If the device is not in Secure Mode when the command is received, 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 the Sector Count register contains a value less than 1 or greater than the maximum number of passwords supported by the device, the command shall not be executed and Abort error shall be returned.

The address contained in the Sector Number, Device/Head, Cylinder Low and Cylinder High registers indicates the starting address of the extent to be placed in Secure Mode. This extent includes all addresses from this address to the maximum address on the device inclusive. If this address is all zeros, the entire device shall be placed into Secure Mode.

Use of the Emergency password is optional. Upon successful completion of this command, the secure state shall reflect Secure Mode RW set, unlocked.

The Emergency password shall be created by the host by asking the user a single of question, what is your mother’s maiden name. The Emergency password shall consist of the user’s response as an ASCII byte stream followed by zero fill to the 512 byte password size.

If an extent of the device is in Secure Mode when this command is received, the command shall not be executed and an Abort error shall be returned.

SECURE ENABLE WP

OPCODE - EAh

TYPE - Optional - Security Mode Feature Set.

PROTOCOL - Non-data command.

INPUTS - The Feature register shall be set to 83h.

NORMAL OUTPUTS - none.

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 is already in secure mode.

PREREQUISITES - The device must not be in Secure Mode.

DESCRIPTION - This command shall set the device into Secure Mode Write Protect. In this mode, the entire device can be read but all write commands shall be rejected.

Once placed in Secure Mode Write Protect state, the device data cannot be written to the device until it is removed from Secure Mode Write Protect by a Disable Secure command.

If the device is in Secure Mode XX state when this command is recieved, it shall be rejected and an Abort error returned.

SECURE LOCK

OPCODE - EAh

TYPE - Optional - Security Mode Feature Set.

PROTOCOL - Non-data command.

INPUTS - The Features register shall be set to 84h.

NORMAL OUTPUTS - none.

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

PREREQUISITES - The an extent on the device must be in Secure Mode and Unlocked.

DESCRIPTION - This command shall lock an extent any time an extent on the device is in secure mode XX, unlocked. If the extent was unlocked with the Features register value 87h, this is the only means of locking the extent. If the extent was unlocked with the Features register value 86h, either this command or powering-down the device shall cause the extent to assume the locked state.

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

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

SECURE STATE

OPCODE - EAh

TYPE - Optional - Security Mode Feature Set.

PROTOCOL - Non-data command.

INPUTS - The Features register shall be set to 85h.

NORMAL OUTPUTS - The Sector Count register specifies the Security Mode state as shown in table S1.

7	6	5	4	3	2	1	0
Secure Enabled RW	Secure Enabled RO	Secure Enabled WP	Unlocked	Lock Flag	Media Not Present		

Table S1 - Security Mode state

Bit 7 - Secure Enabled RW - If set, indicates that an extent on the device has been set in Secure Mode Read/Write.
Bit 6 - Secure Enabled RO - If set, indicates that an extent on the device has been set in Secure Mode Read Only.
Bit 5 - Secure Enabled WP - If set, indicates that the device has been set in Secure Mode WP
Bit 4 - Unlocked - If set, indicates that the extent on the device has been unlocked.
Bit 3 - Lock Flag - If the device is in Secure Mode and this bit is cleared, the Secure Mode extent on device will assume the locked state when powered down. If the device is in Secure Mode and this bit is set, the Secure Mode extent on device can only be locked by issuing a Lock command.
Bit 2 - Media Not Present - Set if the device is a removable media device and no media is present.
Bit 1:0 -reserved.

ERROR OUTPUTS - Aborted Command error if the device does not support the Secure Mode Feature Set.

PREREQUISITES - None.

DESCRIPTION - This command shall return the Secure Mode state of a device that implements the Secure Mode Function Set. Upon completion of the command, the Sector Count register shall contain the Secure Mode state as shown in table S1.

SECURE UNLOCK

OPCODE - EBh

TYPE - Optional - Security Mode Feature Set.

PROTOCOL - PIO data out.

INPUTS - The Features register shall be set to 86h or 87h. The Sector Count register shall be set to 01h.

NORMAL OUTPUTS - none.

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 an extent of the device is not already in Secure Mode.
the device supports the Secure Mode Feature Set and the value set in the Sector Count register is not equal to 01h.

PREREQUISITES - An extent of the device must be in Secure Mode.

DESCRIPTION - This command unlocks an extent on a device in the Secure Mode to allow data transfers.

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

The device shall match the password received with this command with the existing set of valid passwords. If the unlock password matches a password in the established set of passwords, the device shall unlock.

The Features register indicates the required action to relock the extent. If the Features register contains the value 86h, the device shall assume the lock state when powered-down. If the Features register contains the value 87h, the device shall only assume the locked state when the LOCK command is received, that is, the device may be powered-down and back up without assuming the locked state.

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

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

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