



## Quick Admin FAQ

**This document contains Frequently Asked Questions about Quick Admin.**

**Q:** Who are MToken Administrators?

**A:** Help Desk Consultants, Staff at the MToken Distribution Centers, MAIS and MCIT staff with access to Quick Admin are all considered MToken Administrators. MAIS (or other) staff with Admin rights in Authentication Manager are also considered MToken Administrators, but are level two support. Help Desks will not have MTokens available.

**Q:** What will an MToken Administrator do when a user requests an MToken?

**A:**

- If it's a new user, give him or her a new Token and flyer about activating Token.
- If the user left their Token at home, assign a temporary static Tokencode vs. giving him or her a new one.
- If the user has lost his or her Token, mark the Token as lost and assign the user a new Token.
- If the user's Token is expiring, give the user a new Token. The MToken Administrator can assign a Token to the user or refer the user to the MTSC to activate the token.
- If the user is not on campus, verify his or her identity, then mail MToken to user (or contact MAIS Access Services to have the MToken sent out).

**Q:** When would an MToken be disabled?

**A:** If there are too many failed authentication attempts are made with either bad PIN's or bad Tokencodes.

**Q:** What is "Next Tokencode Mode"?

**A:** When a Token is in this mode, the user is prompted for a second consecutive Tokencode after a correct code is entered – providing further proof that the user actually has possession of their token.

**Q:** What is the difference between a Passcode and a Tokencode?

**A:** A Passcode is a PIN followed by a Tokencode. A Tokencode is the changing code (a pseudo-random number) generated by a token, which is displayed on the hardware token's LCD.

**Q:** What is a PIN?

**A:** Personal Identification Number. The (alpha) numeric set of characters that identifies a user as the authorized holder of a particular MToken. These are only used by MAIS staff.

**Q:** If a user calls about a lost token, what should the Administrator do?

**A:** Determine if the token is 'temporarily' lost or unrecoverable. This determines the difference between arranging for a replacement token or just supplying a Temporary Static Tokencode.

**Q:** If the lost token could not be recovered, what administrative actions should be taken?

**A:** The lost token should be unassigned from the user (disabling it from possible login with the assigned User ID). If it is certain that the token is unrecoverable, it can be deleted from the database. The user should then be directed to an MDC to pick up a replacement MToken. The MToken can be activated for the user by the consultant at the MDC.

**Q:** A user calls stating that their MToken is broken. What should the user do?

**A:** The user can call a Help Desk, who will then assign a temporary password (HD will mark Token as lost in order to do this) which will work until the user has an opportunity to visit an MDC to get a new Token. The MDC would unassign the broken token and assign the new Token.

**Q:** Where would a user send a broken Token?

**A:** To MAIS Access Services or an MDC.

**Q:** What should a department do when a person's appointment is terminated?

**A:** Collect their MToken(s) from the departing staff, that either no longer have access to a system that requires Two Factor Authentication or are leaving the University. These Tokens can be re-used by other staff, but only after they have been unassigned.

**Q:** What should an MToken Administrator do if a user calls and says they found a previously "lost (unrecoverable)" MToken?

**A:** the MToken Administrator should advise the user to return the lost MToken to an MToken Distribution Center and continue to use the new MToken that was assigned. If a new MToken has not yet been assigned to replace the lost MToken, the Administrator can re-enable the previously disabled MToken. Please refer to the "How to Enable a Previously Disabled MToken" procedure.