



MToken Administrator Lost Temporary Static Tokencode Procedure

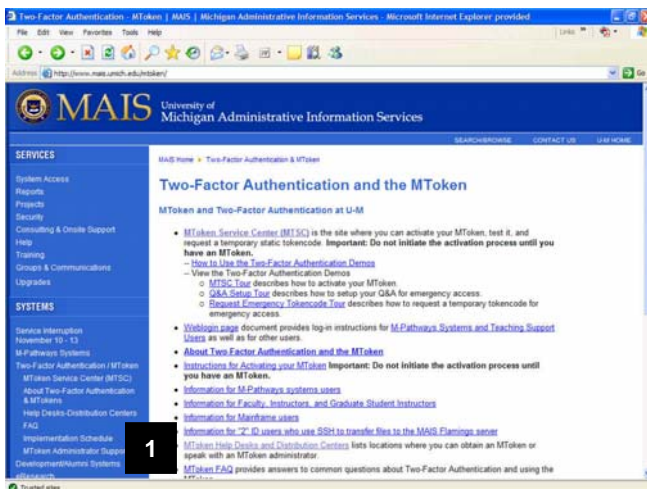
If a user calls an MToken Administrator claiming to have lost their MToken Temporary Static Tokencode, the MToken Administrator can assign a new Temporary Static Tokencode, following this procedure. If another MToken Administrator calls, they will need to contact Access Services to have the password reset.

This process is done using Quick Admin Authentication Manager. Log on to Quick Admin here:
<http://www.mais.umich.edu/mtoken/>

Important Information

 Access to Quick Admin is limited to Tier 1 support staff, which includes all MToken Administrators.

MAIS Web Site



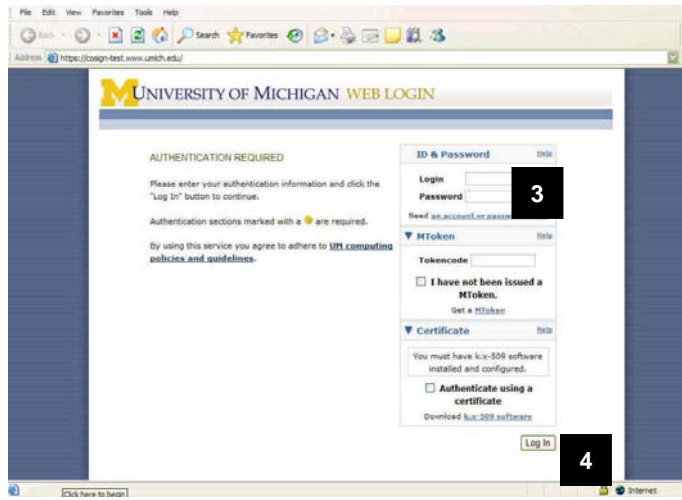
1. From the MAIS Web site, click the link for **MToken Administrator Support**.

MToken Administrator Support



2. Click the link for **MToken Quick Admin**.

University of Michigan CoSign Login

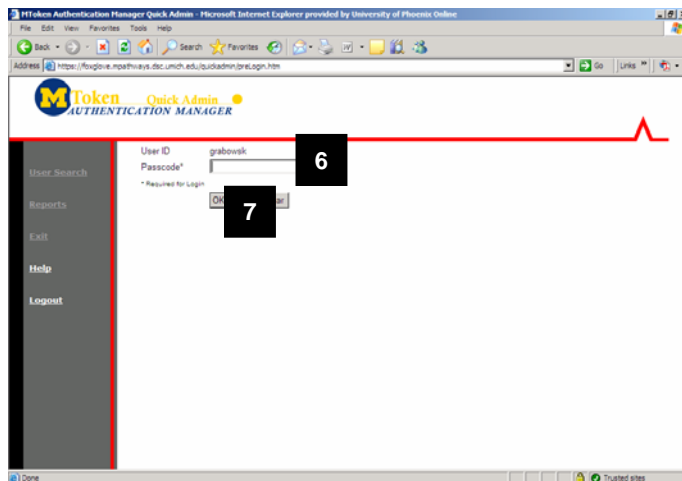


3. Log in with your unqname and Kerberos password.
4. Click **Log In**.

Note: You do not need to enter a Tokencode at this point. If you do, you will have to enter a new code at the Quick Admin login screen.

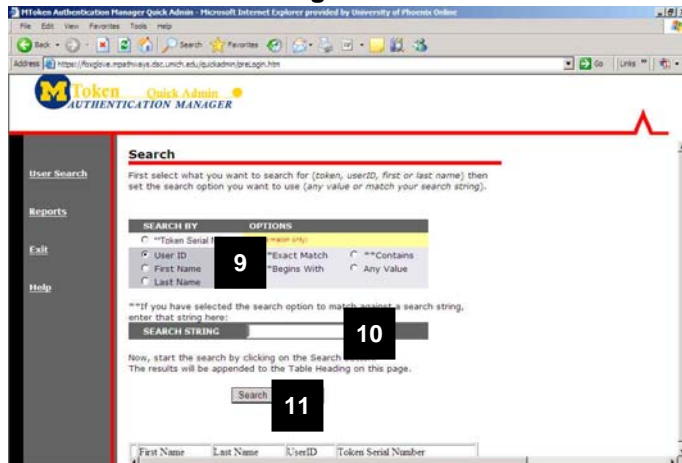
Note: You cannot use the same Tokencode twice.

MToken Quick Admin Login



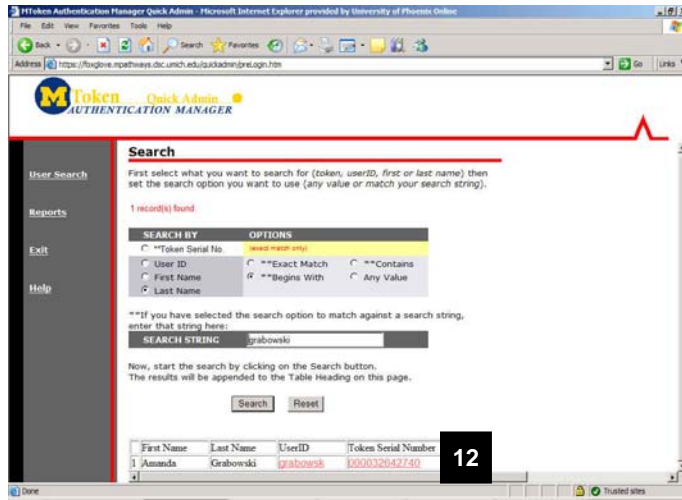
5. Verify that your **User ID** has populated correctly.
6. Enter your **Tokencode** in the Passcode field, which is the number displayed on the front of your MToken.
7. Click **OK**.

Quick Admin Search Page



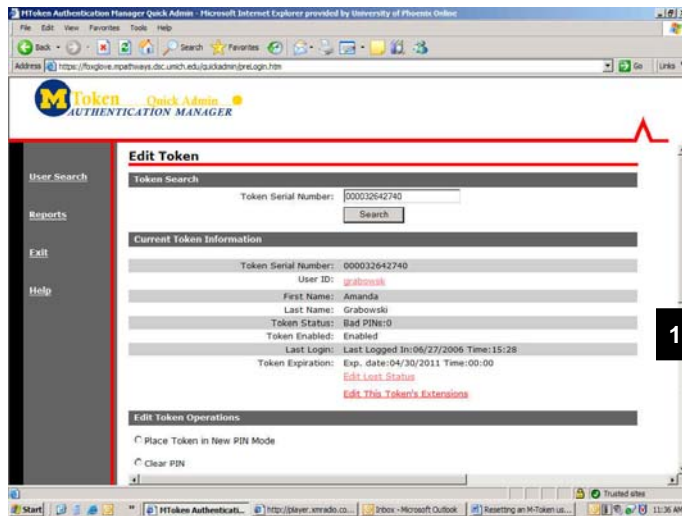
8. If you have logged in properly, you will see the main Search screen.
9. Decide which search parameter you would like to use (User ID, First Name or Last Name) and select the appropriate radio button.
10. Enter the corresponding parameter.
11. Click **Search**.

Quick Admin Search Results



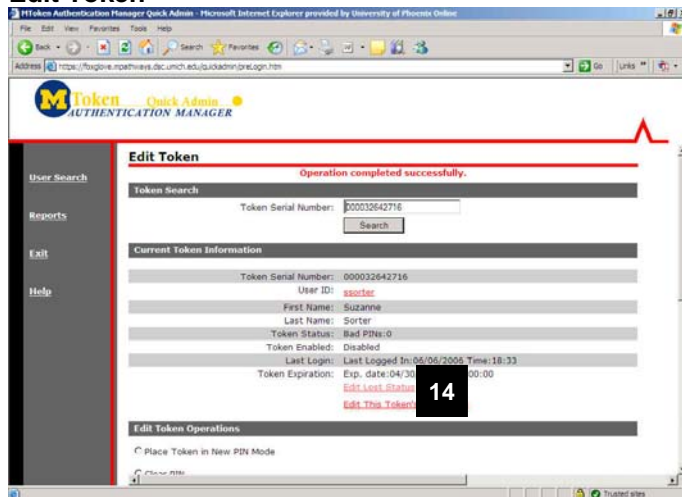
12. From the search results, click on the Token Serial Number.

Edit Token



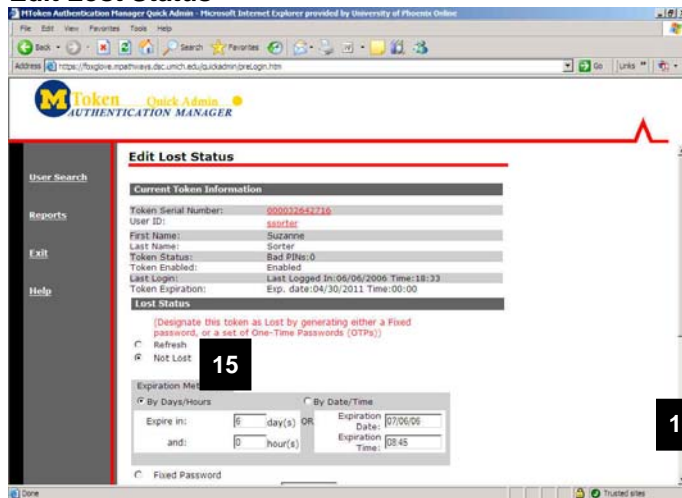
13. Scroll down.

Edit Token



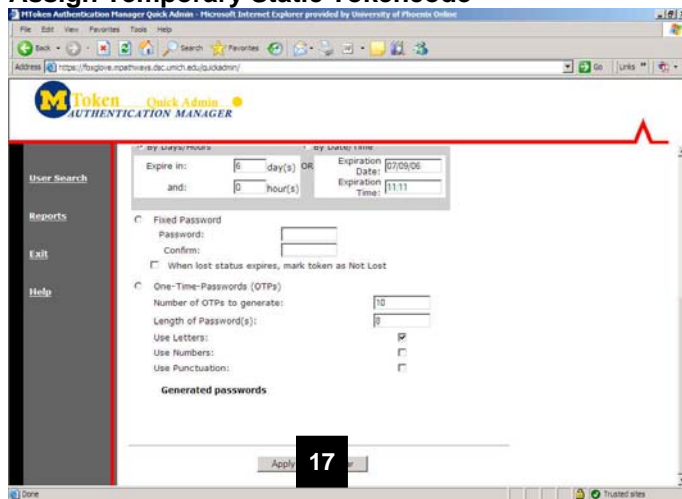
14. Click **Edit Lost Status** to assign a Temporary or Fixed Static Tokencode.

Edit Lost Status



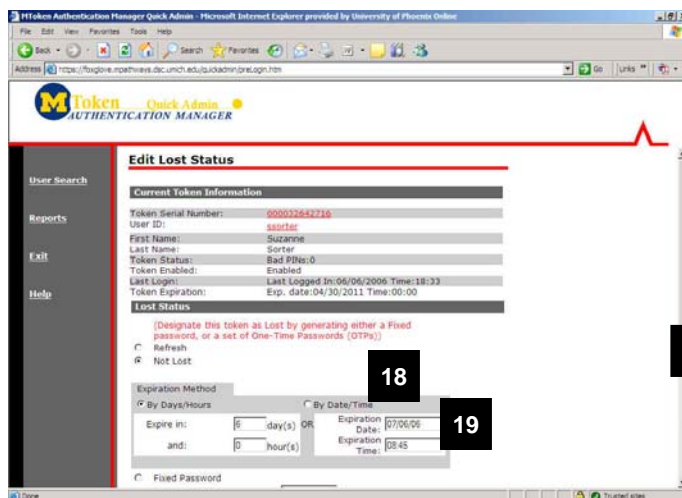
- 15. Accept the default of Not Lost.
- 16. Scroll down.

Assign Temporary Static Tokencode



- 17. Click **Apply**.

Assign Temporary Static Tokencode



- 18. Click the By Date/Time radio button.
- 19. Fill in the expiration date and time with the following business day at 09:00am. These fields will NOT default.
- 20. Scroll down.

Assign Temporary Static Tokencode

The screenshot shows the MToken Authentication Manager Quick Admin interface. The main content area is titled "By Days/Hours" and "By Date/Time". Under "By Days/Hours", there are fields for "Expire in:" (0 day(s) and 0 hour(s)) and "and:". Under "By Date/Time", there are fields for "Expiration Date:" (07/06/06) and "Expiration Time:" (08:56). The "Fixed Password" section is selected, showing "Password:" and "Confirm:" fields. A checkbox labeled "When lost status expires, mark token as Not Lost" is checked. Below this, there are options for "One-Time-Passwords (OTPs)" including "Number of OTPs to generate:" (10), "Length of Password(s):" (8), and checkboxes for "Use Letters:", "Use Numbers:", and "Use Punctuation:". A "Generated passwords" section is visible at the bottom. A sidebar on the left contains "User Search", "Reports", "Exit", and "Help". A "21" callout is next to "Reports", "24" is next to "Exit", "22 & 23" are next to the password fields, and "25" is next to the "Apply" button.

21. Click **Fixed Password**.
22. Type in a random 6 digit numeric code as a fixed password.
23. Re-type the password in the Confirm field.

Note: If you need assistance generating a random 6 digit password, click here to access a Web site that will automatically generate passwords for you, based on selected parameters:
<http://www.winguides.com/security/password.php>

24. Check the **"When lost status expires, mark token as Not Lost"** checkbox.

Note: If the user needs a temporary password for more than one business day, click either the **By Days/Hours** the **By Date/Time** radio button. Enter the corresponding parameters.

25. Click **Apply**.

Note: The Temporary Static Tokencode will expire at 9:00 AM the next business day unless otherwise specified. Token status will change to "Not lost" at this time.

MToken Service Center (MTSC)

The screenshot shows the MToken Service Center (MTSC) user interface. The main content area is titled "Home" and contains two main sections: "MTokens" and "Emergency Access - Forgotten MToken". The "MTokens" section lists the following steps: "Request an Activation Code", "Activate an MToken", "Test Your MToken", and "Replace an Expiring MToken". The "Emergency Access" section lists the following steps: "Set up Q & A Authentication" and "Request Emergency Access". A "Resources" sidebar is on the right, containing links to "Home Security Tour", "MToken - The U-IT Two-Factor Authentication System", and "Help". The footer contains "Copyright © 2001 - 2003 RSA Security Inc. All rights reserved."

26. Have the user go to the MToken Service Center to test their TST by clicking **Test Your MToken**. The user can also test their TST by logging into the desired application.