

Lost or Forgotten eTokens Step by Step Procedure

This section provides instructions and screen shots describing the typical functions that a department administrator may expect to encounter. In order to perform these tasks, the department administrator (DA for short), must have the following prerequisites:

1. an eToken issued to themselves by the ITS eToken administrator.
2. the desktop computer used to run the SafeNet Authentication Manager (SAM) must run a current Windows operating system.

The Internet Explorer web browser must be used to interact with SAM and must be configured as described in the Technical Information section.

User Assistance Procedures

Users may occasionally lose or forget their eToken. The recommended procedure for lost and/or forgotten tokens is to replace the eToken using SAM, and then enroll a new token to that user. The lost or forgotten eToken will be labelled as lost in the system and remains as such until the token is found and returned to the Department Administrator.

Temporarily misplaced or forgotten eTokens are to be returned to the DA as soon as the token is located, so that it may be initialized and re-assigned at a later date.

Replacing a lost/forgotten eToken

1. Access SAM by inserting your eToken, open Internet Explorer, and access the URL:

<https://ekey.utoronto.ca/sammanage>

2. You will notice your UTORid in the upper right. Select 'Helpdesk'.
3. Connect a new unassigned/blank eToken
4. 'Search for': Tokens by user. Enter UTORid of User Select 'Go'.
5. Highlight the account name of the user with the lost/forgotten eToken. Select the 'replace' option from the drop down menu.

The screenshot shows the SafeNet Authentication Manager interface. The top header includes the SafeNet logo, the text "SafeNet Authentication Manager", and "UTORid of DA" on the right. A navigation sidebar on the left contains links for Helpdesk, Deployment, Inventory, Reports, and Downloads. Below the sidebar, there are search fields for "Domain" (set to "UTORARBOR.UTORAD."), "Search for:", "Tokens by user", "Search criteria:", "UTORid of User", and "And". A "Go" button is at the bottom of the sidebar.

The main content area displays a table with the following data:

Account Name	Type	ID	Status
UTORid of User	SafeNet eToken 510x	0x01f51715	Enabled,Normal

Below this table is another table with columns "Application", "Expiration Date", and "Details":

Application	Expiration Date	Details
Connector for Microsoft CA	5/29/2017	Detail
Connector for P12 Certificate Import	N/A	Detail

At the bottom of the main area, there are buttons for "Reset Pwd", "Revoke", "Unassign", "Unlock", and a "More Actions..." dropdown menu. The dropdown menu is open, showing options: "More Actions...", "Temp Logon", "Disable", and "Replace" (which is highlighted in blue).

6. Select "lost" from drop down menu citing reason for replacement (please note: all lost and/or forgotten are to be labelled lost until returned)
7. Select the 'Run' button.

The screenshot shows the "Replace a Smartcard or USB Token" wizard in the SafeNet Authentication Manager. The top header is the same as the previous screenshot. The main content area displays the following information:

Name: UTORid of User Serial Number: 0x01f51715

Replace a Smartcard or USB Token

[Customize replacement](#)

Ensure that the new token is connected

Warning: If the token is initialized, all data on it will be erased.

Reason for replacement: Initialize token

- Select reason for replacement...
- Damaged
- Lost
- Upgrade

At the bottom of the wizard, there are buttons for "Back", "Run", and "Done".

Below the wizard, there is a text box containing the instruction: "Provide the user with a new token, and revoke the current token".

8. Select the 'Done' button. The new eToken is now ready for the user.