

Replacing Damaged 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 encounter a defective or damaged eToken. The recommended procedure for these is to replace the token using SAM, and enroll a new token to that user. The damaged eToken will be labelled as damaged in the system and is to be removed from circulation by the DA.

Damaged eTokens should be stored and secured by all Department Administrators.

Replacing a Damaged 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. 'Search for': Connected tokens.
4. Highlight the account name of the user with damaged the eToken. Select the 'replace' option from the drop down menu.
5. Connect new "unassigned" eToken

The screenshot shows the SafeNet Authentication Manager interface. The top header includes the SafeNet logo and the text 'SafeNet Authentication Manager' and 'UTORid of DA'. On the left is a navigation sidebar with options: Helpdesk, Deployment, Inventory, Reports, and Downloads. Below the sidebar is a 'Domain' section with 'UTORARBOR.UTORAD.' and a 'Search for:' field containing 'Connected tokens'. The main area displays a table of tokens:

Account Name	Type	ID	Status
UTORid of DA	SafeNet eToken 510x	0x01f516f2	Enabled,Normal
UTORid of User	SafeNet eToken 510x	0x01f51715	Enabled,Normal

Below the table is another table with columns 'Application', 'Expiration Date', and 'Details':

Application	Expiration Date	Details
Connector for Microsoft CA	6/1/2017	Detail
Connector for P12 Certificate Import	N/A	Detail

At the bottom of the main area is a 'Recover Certificates' button. Below the main area is a row of buttons: 'Reset Pwd', 'Revoke', 'Unassign', 'Unlock', and a 'More Actions...' dropdown menu. The dropdown menu is open, showing options: 'More Actions...', 'Disable', and 'Replace' (which is highlighted in blue).

6. Select "damaged" from drop down menu citing reason for replacement
7. Select the 'Run' button.

The screenshot shows the 'Replace a Smartcard or USB Token' wizard in the SafeNet Authentication Manager. The top header includes the SafeNet logo and the text 'SafeNet Authentication Manager' and 'UTORid of DA'. On the left is a navigation sidebar with options: Helpdesk, Deployment, Inventory, Reports, and Downloads. The main 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.

Initialize token

Reason for replacement: Select reason for replacement...

The dropdown menu for 'Reason for replacement' is open, showing options: 'Select reason for replacement...', 'Damaged' (highlighted in blue), 'Lost', and 'Upgrade'.

At the bottom of the main area are three buttons: 'Back', 'Run', and 'Done'.

Below the main area is a footer bar with the text: 'Provide the user with a new token, and revoke the current token'.

8. Select the 'Done' button. The old token is now 'damaged' and new eToken is ready for the user.