

Unassign User Step-by-Step Procedures

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.

Unassigning a User

1. Take possession of the user's eToken.
2. Access SAM by inserting your eToken, open Internet Explorer, and access the URL:

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

3. You will notice your UTORid in the upper right. Select 'Helpdesk'.
4. 'Search for:' Connected tokens.
5. Connect the user's token to your computer - so there will be two eTokens connected. Select 'Go'.
6. Highlight the account name of the user to be unassigned. Select the 'Unassign' button.

The screenshot shows the SafeNet Authentication Manager (SAM) web interface. The top header includes the SafeNet logo and the text "SafeNet Authentication Manager". On the right side of the header, there is a field for "UTORid of DA" and an "About" link. The main content area is divided into a sidebar on the left and a main panel on the right. The sidebar contains navigation options: "Helpdesk", "Deployment", "Inventory", "Reports", and "Downloads". Below these is a "Domain" field with the value "UTORARBOR.UTORAD." and a "Search for:" field with the value "Connected tokens". A "Go" button is located below the search field. The main panel displays a table of connected tokens. The table has columns for "Account Name", "Type", "ID", and "Status". There are two rows: "UTORid of DA" and "UTORid of User". Below the table, there is a section for "Application", "Expiration Date", and "Details". There are two rows: "Connector for Microsoft CA" and "Connector for P12 Certificate Import". A "Recover Certificates" button is located below this section. At the bottom of the interface, there is a row of buttons: "Reset Pwd", "Revoke", "Unassign", "Unlock", and "More Actions...". The "Unassign" button is circled in red.

Account Name	Type	ID	Status
UTORid of DA	SafeNet eToken 510x	0x01f516f2	Enabled,Normal
UTORid of User	SafeNet eToken 510x	0x01f51708	Enabled,Normal

Application	Expiration Date	Details
Connector for Microsoft CA	6/11/2017	Detail
Connector for P12 Certificate Import	N/A	Detail

Buttons: Reset Pwd, Revoke, **Unassign**, Unlock, More Actions...

7. Select the 'Run' button.

The screenshot displays the SafeNet Authentication Manager web interface. At the top left is the SafeNet logo and the text 'SafeNet Authentication Manager'. At the top right, it shows 'UTORid of DA' and an 'About' link. A vertical sidebar on the left contains navigation buttons: 'Helpdesk', 'Deployment', 'Inventory', 'Reports', and 'Downloads'. The main content area is titled 'Unassign a Token' and displays the following information: 'Name: UTORid of User' and 'Serial Number: 0x01f51708'. Below this information is a large empty rectangular area. At the bottom right of this area are three buttons: 'Back', 'Run' (which is highlighted with a blue border), and 'Done'. Below the main content area is a grey footer bar with the text: 'Disassociate a token from the user, and revoke the credentials on it'.

8. On completion, select the 'Done' button.