|  |
| --- |
| PAM (Hitachi ID Privileged Access Manager) User documentation |
| 7/3/2014 |
| IAM Team |

Contents

[Document overview 2](#_Toc395865211)

[User Requestor Access 2](#_Toc395865212)

[Prerequisites 2](#_Toc395865213)

[Login 2](#_Toc395865214)

[Request Access 3](#_Toc395865215)

[Service Owner Access 7](#_Toc395865216)

[Prerequisites 7](#_Toc395865217)

[Login 7](#_Toc395865218)

[Approve Requests 7](#_Toc395865219)

[Request Access 10](#_Toc395865220)

## Document overview

**Privileged Access Manager (PAM) enterprise service** will be implemented at UBC to create secure access to privileged accounts. It works by regularly randomizing privileged passwords on workstations, servers, network devices and applications. Random passwords are encrypted and stored on at least two geographically dispersed replicated credentials vaults. To start with, we will manage the root/sysadmin account on Linux and Administrator account on Windows. This will replace various existing password management software, provide a centralized password management system, workflows and delegation to these privileged accounts.

This document is intended to provide the steps required to use basic functionality in PAM, for both the User requesting access and the Service Owner.

## User Requestor Access

### Prerequisites

The following prerequisites are required to use the PAM application:

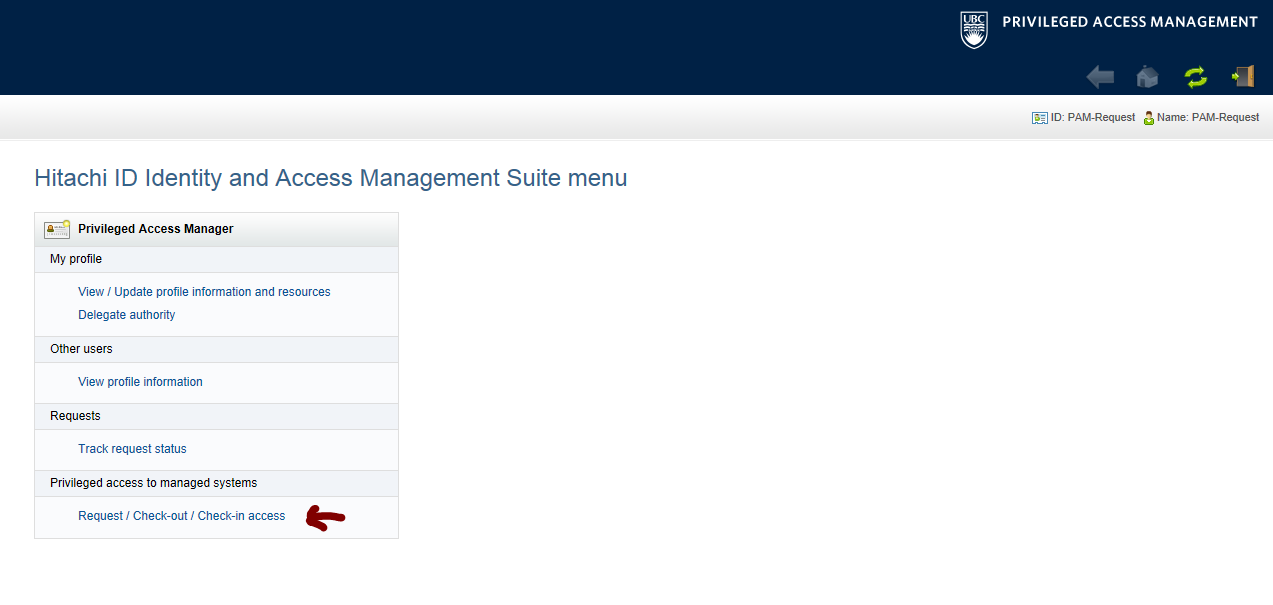
* An Enterprise Active Directory (EAD) admin account
* A workstation with Internet Explorer

### Login

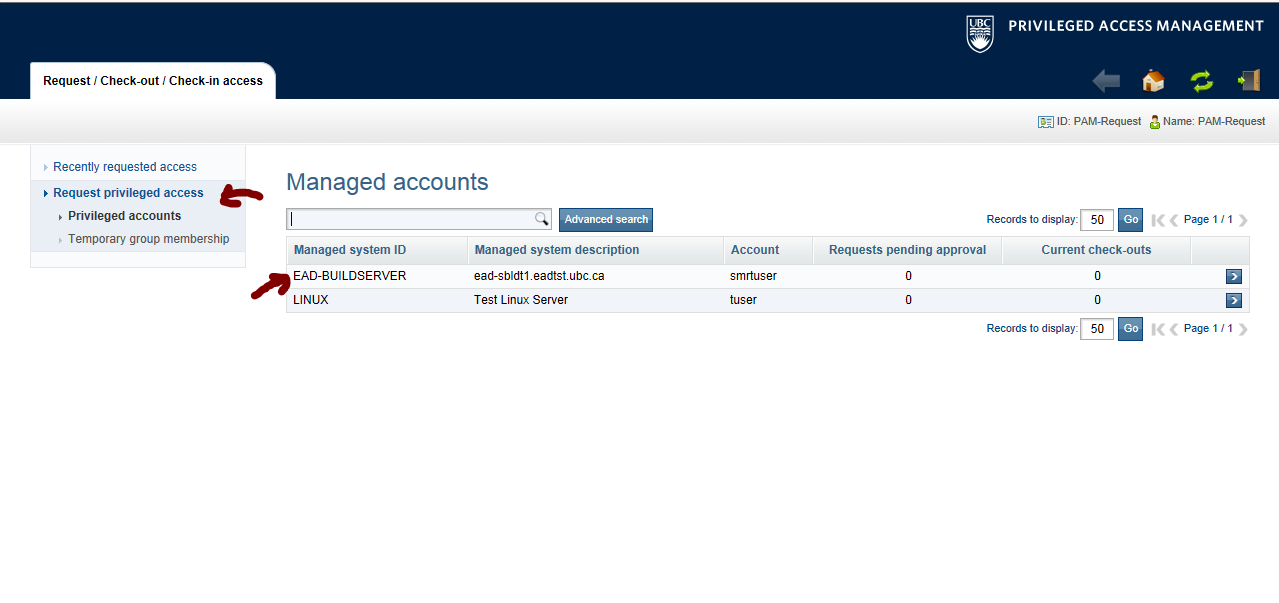
Log into [pam.it.ubc.ca](file:///C:\Users\nmas\Documents\pam.it.ubc.ca) using your EAD Admin account.

### Request Access

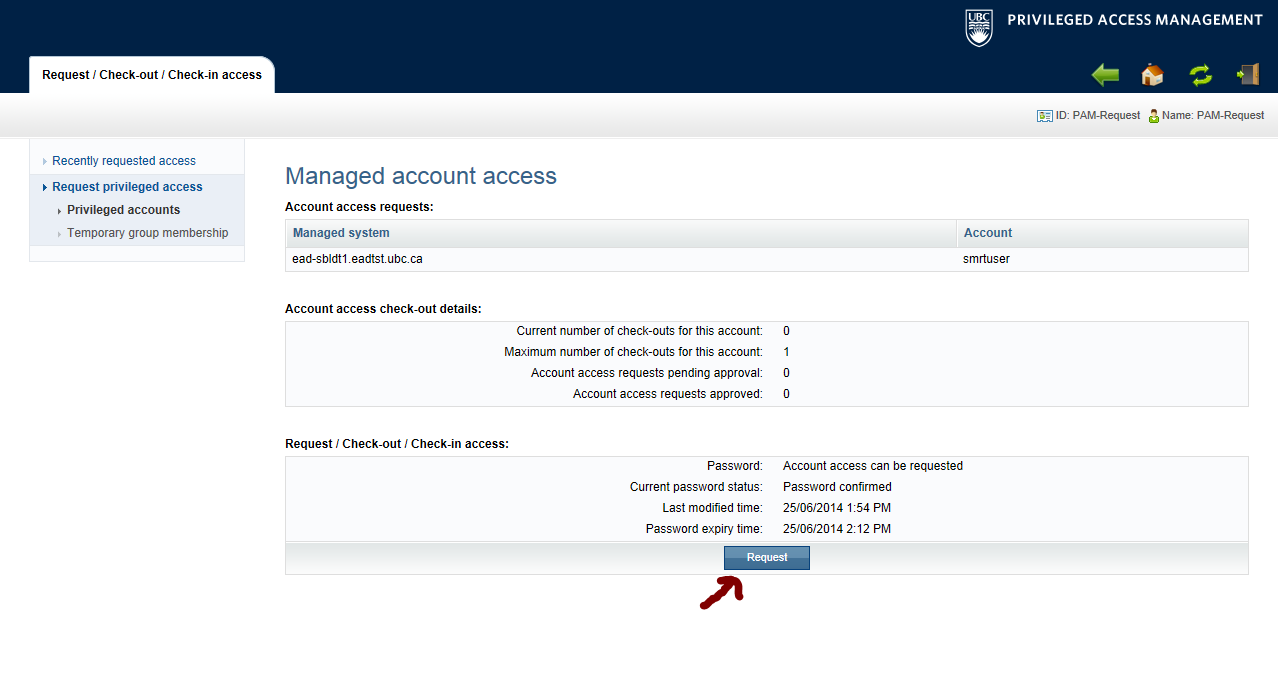
1. Select **Request/Check out/Check in access** from the menu



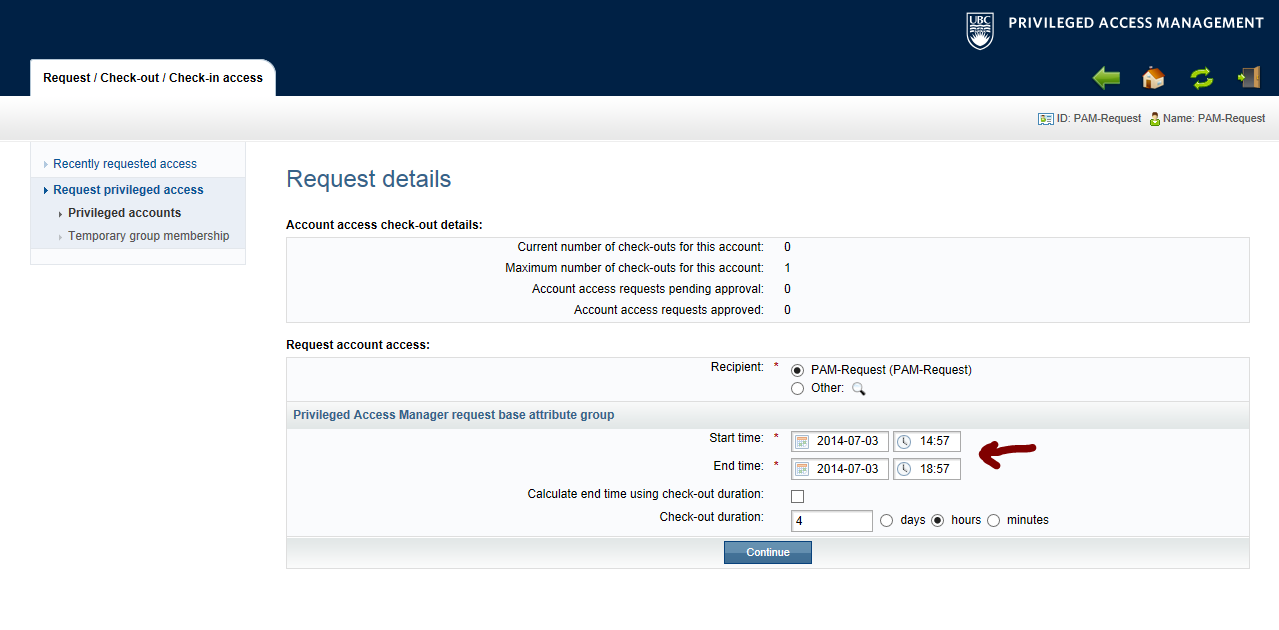
1. Select **Request Privileged access** from the menu on left, then select the server you need to access



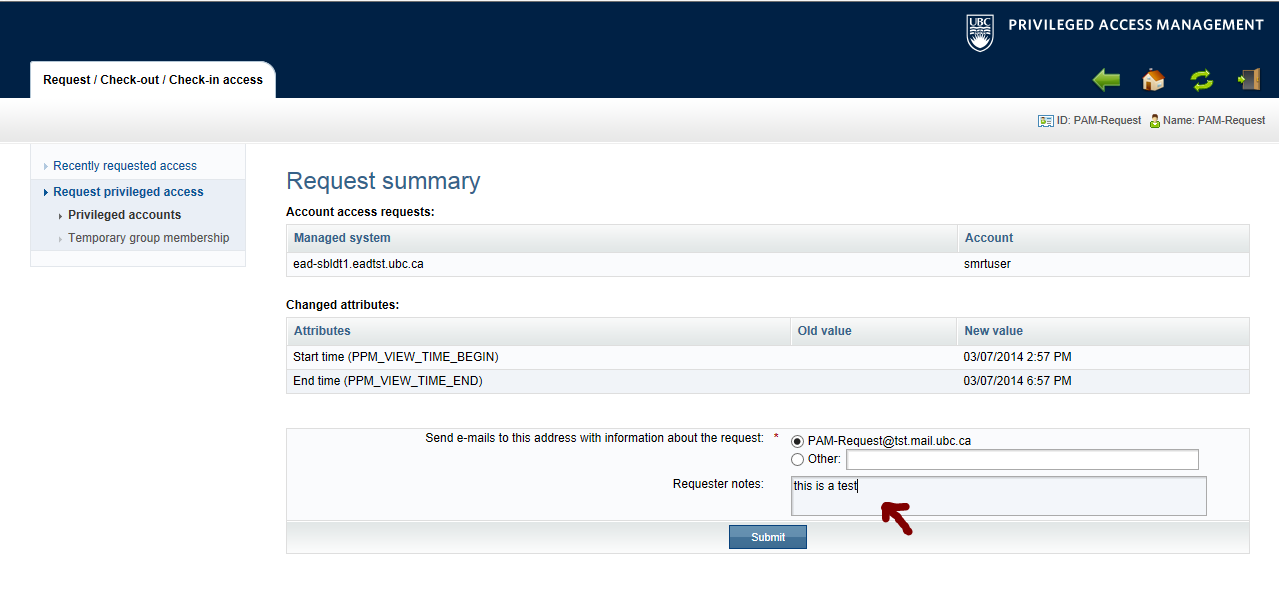
1. Click the **Request** button



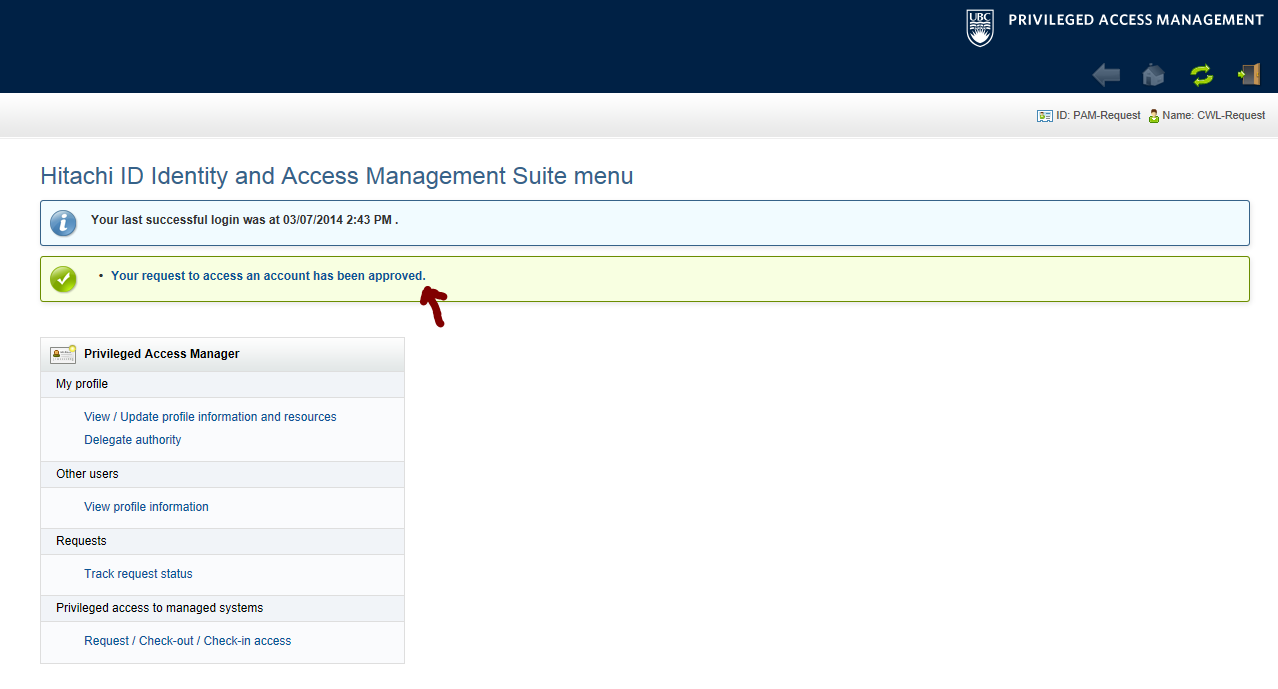
1. Enter the **date/time** for access and click the **Continue** button



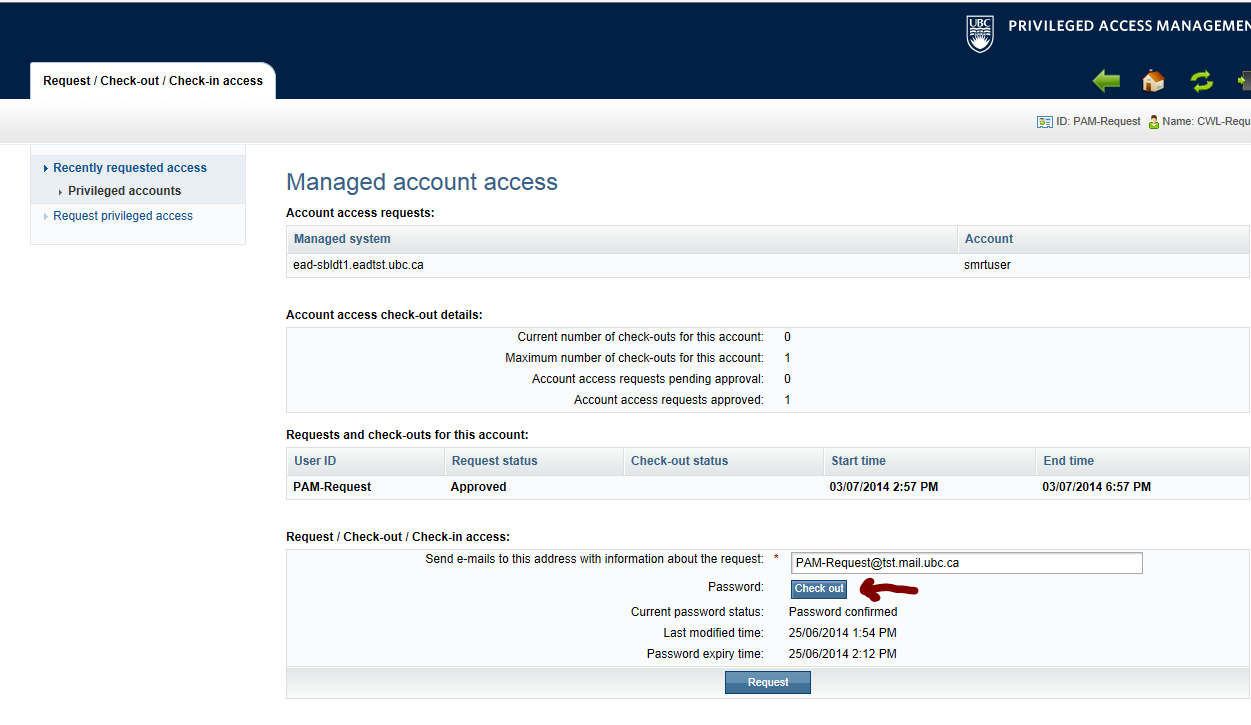
1. Enter a **Requestor Note** and click the **Submit** button



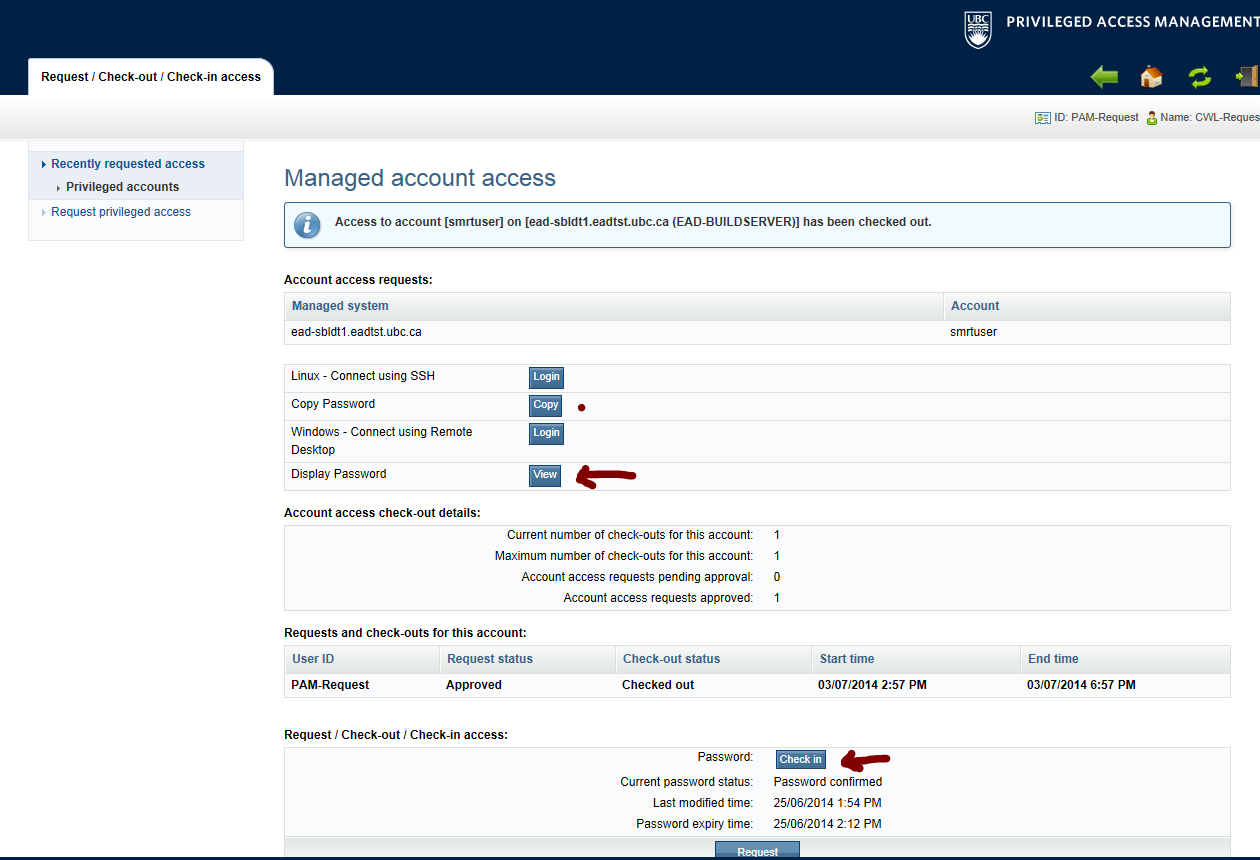
1. The request has been sent for approval. You will receive an email notification for your request and once approved you will receive a confirmation email.
2. Select **Your request to access an account has been approved**



1. Select **Check out** password button



1. From this screen you can **Display, Copy** password or **Login**. Once work is completed you can **check in** the password.



## Service Owner Access

### Prerequisites

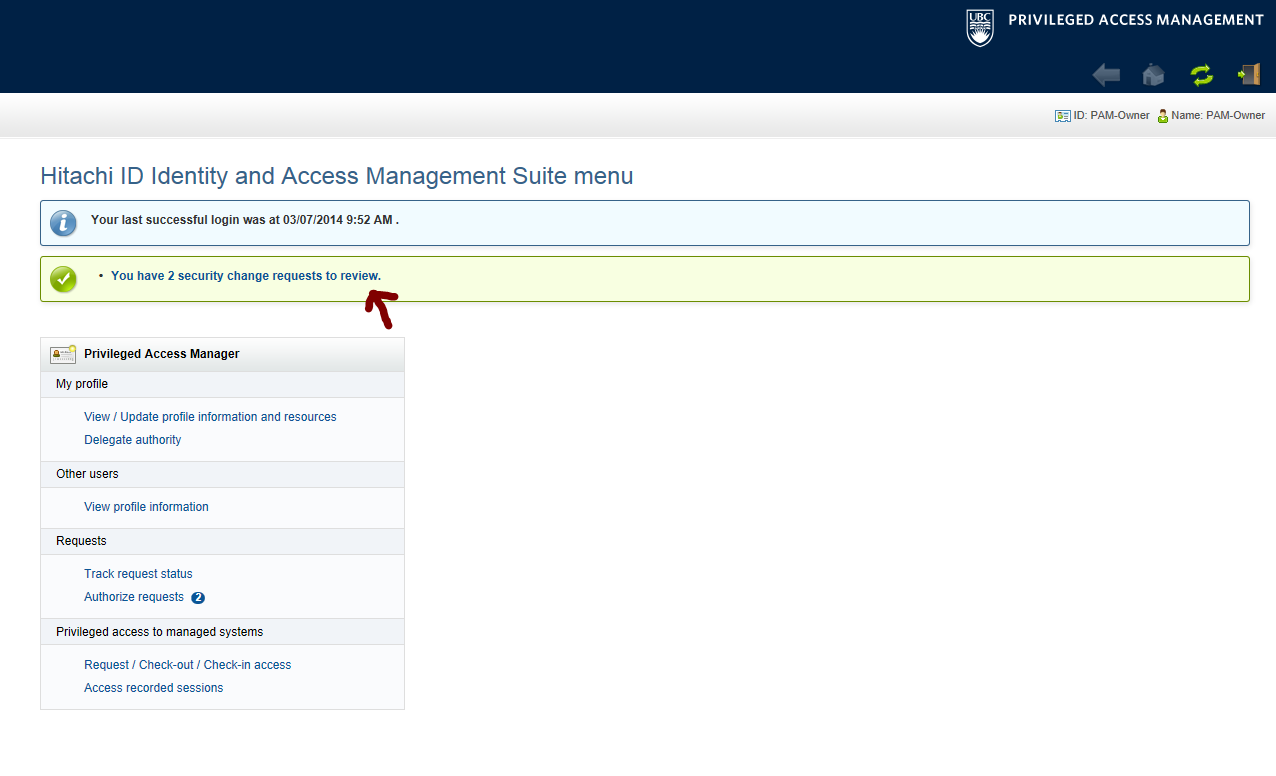
The following prerequisites are required to use the PAM application:

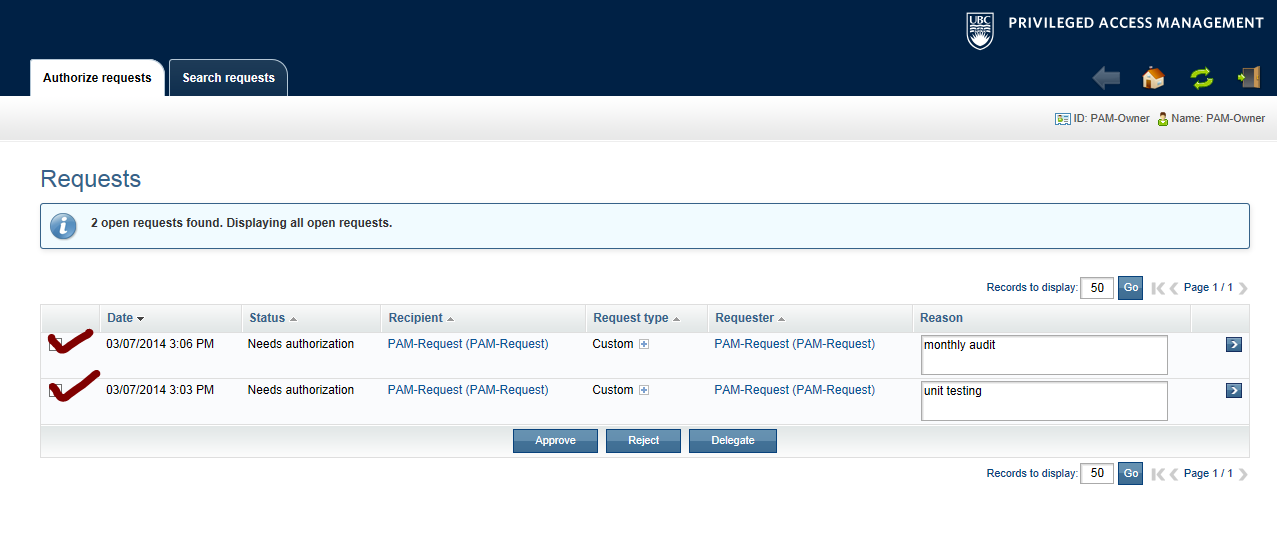
* An Enterprise Active Directory (EAD) admin account
* Your Server integrated with PAM and delegated (contact <http://web.it.ubc.ca/forms/iam> for more information)
* A workstation with Internet Explorer

### Login

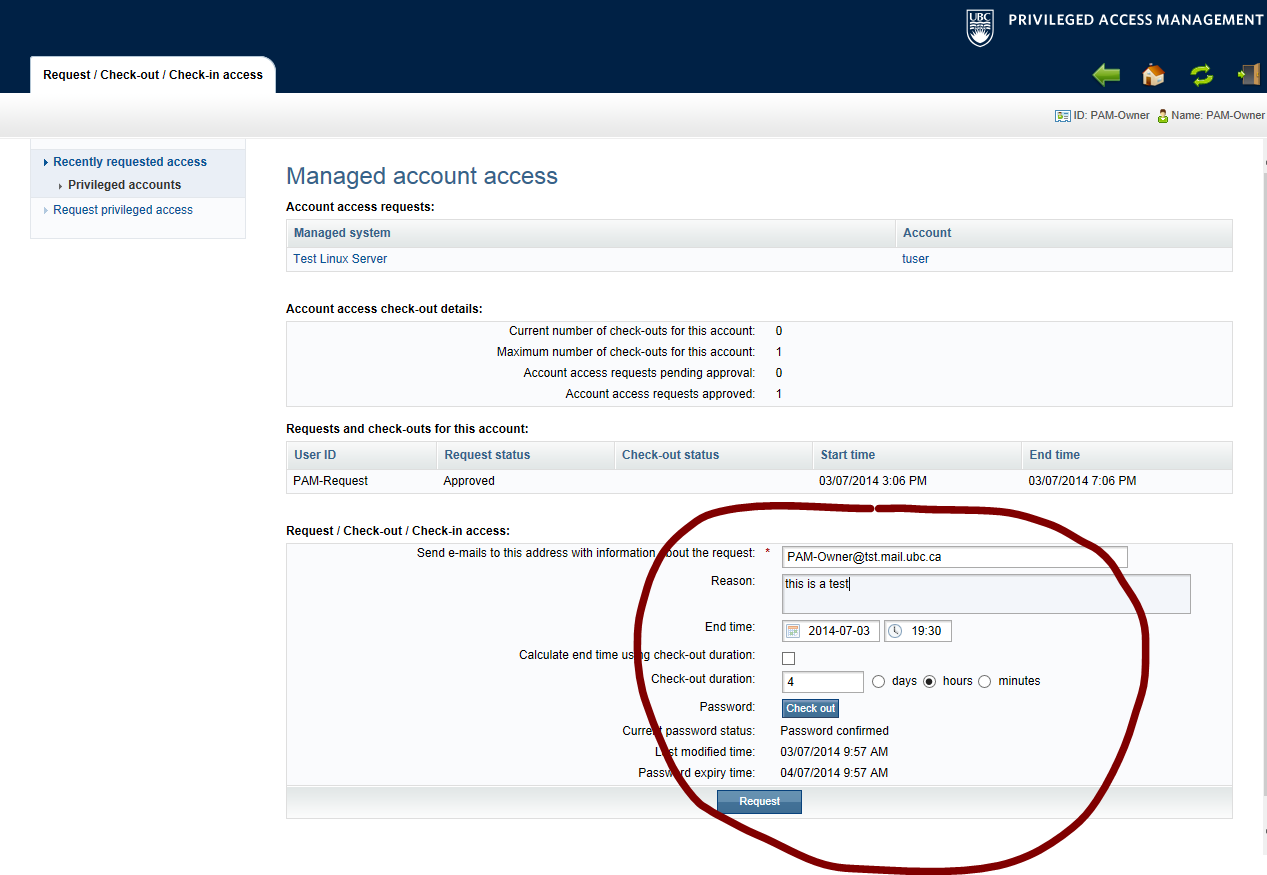
Log into pam.it.ubc.ca using your EAD Admin account.

### Approve Requests

1. Select to review security change requests
2. Select access requests and click the **Approve** button. Enter Reason field, if needed.



1. Review the Requestor workflow for steps to complete. There is no approval process required for the Service Owner.



### Request Access

Service owners can automatically check out password to accounts they manage without going through workflow. Follow this instructions to check out a password.

1. Select **Request/Check out/Check in access** from the menu
2. Select the Server you want to access
3. Complete the **Reason field,** enter a **date/tim**e for access and click the **Checkout** button

