

Job Aid to access Linux/Solaris servers via PAM

Summary

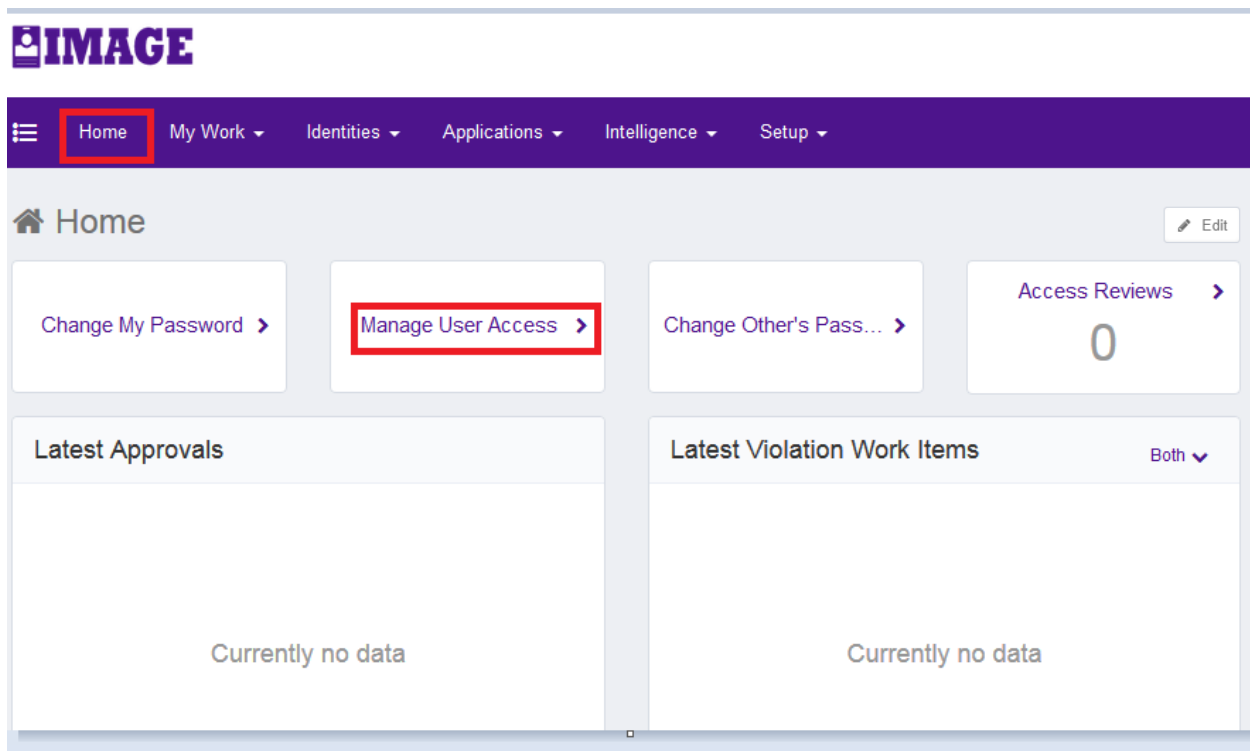
This job aid will provide the instructions to the SA teams on how to access PAM as well as how to SSH to the Linux servers via PAM using the PAM managed 'root' account.

Steps to be performed

➤ Request PAM role from IMAGE

Login into IMAGE <https://sso.secure.fedex.com/image>

Navigate to Home → Manage User Access*



**If Manage User Access is not available on your Home screen, please click Edit in the upper right corner of the screen and then click Add Card to add it.*

On the Manage User Access page:

Click on Select Users tab → enter your FedEx ID and click Search → select your Fedex ID in the search results as shown below.



 Home

 Laxmi Swetha Po... 

Manage User Access

 Select Users

Select Access

Review & Submit



 Laxmi Swetha Potana

Showing 1-1 of 1

 All 

 Laxmi Swetha Potana

Username: 5000359
Manager: Trey Ray



 Laxmi Swetha Potana

Showing 1-1 of 1

Click on Select Access tab → search for the entitlement/role – **ito_sa_implementation**

Select the role in the search results.



 Home

My Work 

Manage User Access

Select Users

Select Access

Add Access 

 ito_sa_implementation

 Laxmi Swetha Potana

Showing 1-1 of 1

 ito_sa_implementation

Grants access to ITO-SA-IMPLEMENTATION SA Image Group

Type: Role Owner: Scott D. Burton Risk: 

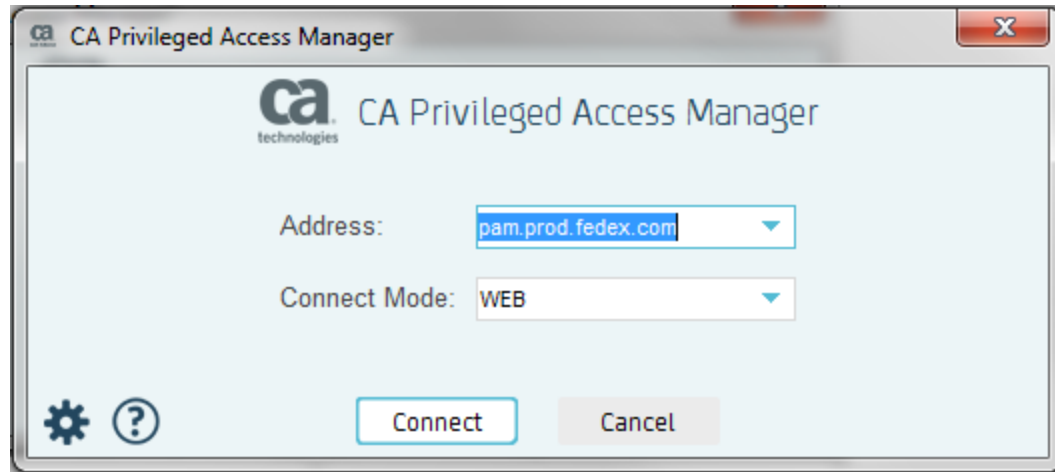
Click on Review and Submit tab → Review the role information, enter a Comment/Reason for requesting the role, and Click on Submit as shown below.

The screenshot shows the IMAGE (Identity Management Access) web application interface. At the top, there is a purple header bar with the IMAGE logo on the left and the FedEx logo on the right. Below the header, a navigation bar contains 'Home' and 'My Work' links. The main content area is titled 'Manage User Access'. It features three tabs: 'Select Users', 'Select Access', and 'Review & Submit' (which is active and highlighted in purple). Below the tabs, a green button labeled 'Laxmi Swetha Polana' is visible. The 'Add Access' section shows a search for 'ito_sa_implementation'. Below this, a table displays the role information: 'Type: Role', 'Owner: Scott D. Burton', and 'FDX-ICA-ADMINIS'. A 'Risk: 0' indicator is shown below the table. At the bottom of the interface, there are 'Cancel' and 'Submit' buttons.

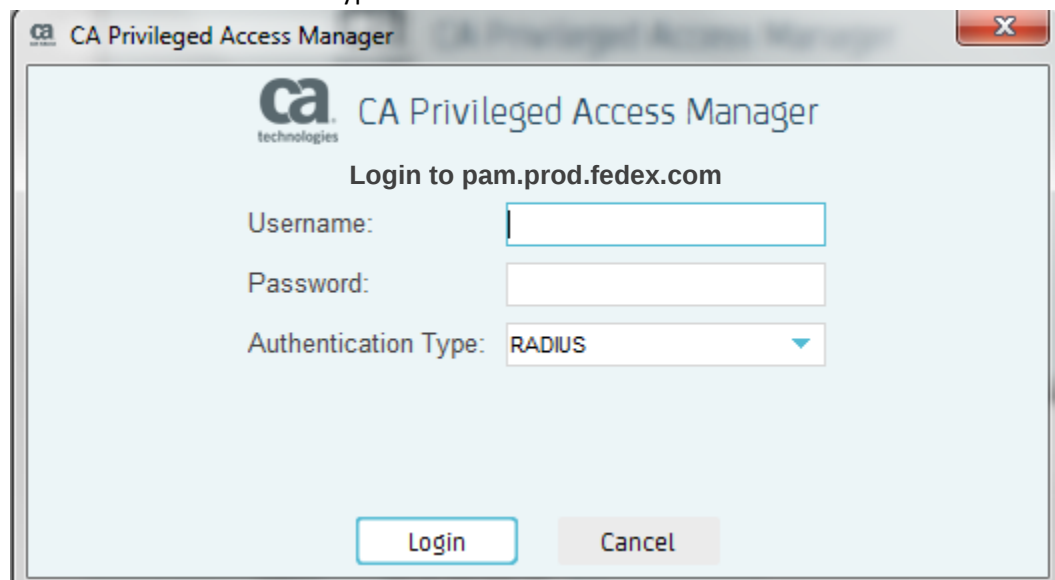
**After manager approvals, your PAM access ready and provisioned.*

➤ How to client Install & Logging into PAM

1. Open a browser and enter <https://esso.secure.fedex.com/infosec/pam/pamclients.phtml>
2. Select the client based on your operating system
3. Once the .exe has download, open it and begin installation
 - a. Select Next then read/accept the License Agreement
 - b. Select Typical installation
 - c. Choose your desired folder and select install
 - d. Choose between rebooting now or later
 - e. Launch the CA PAM Client
4. For address: *Provided by GRUNT search* (i.e pam.prod.fedex.com)
Connection Mode: Web and click "Connect"



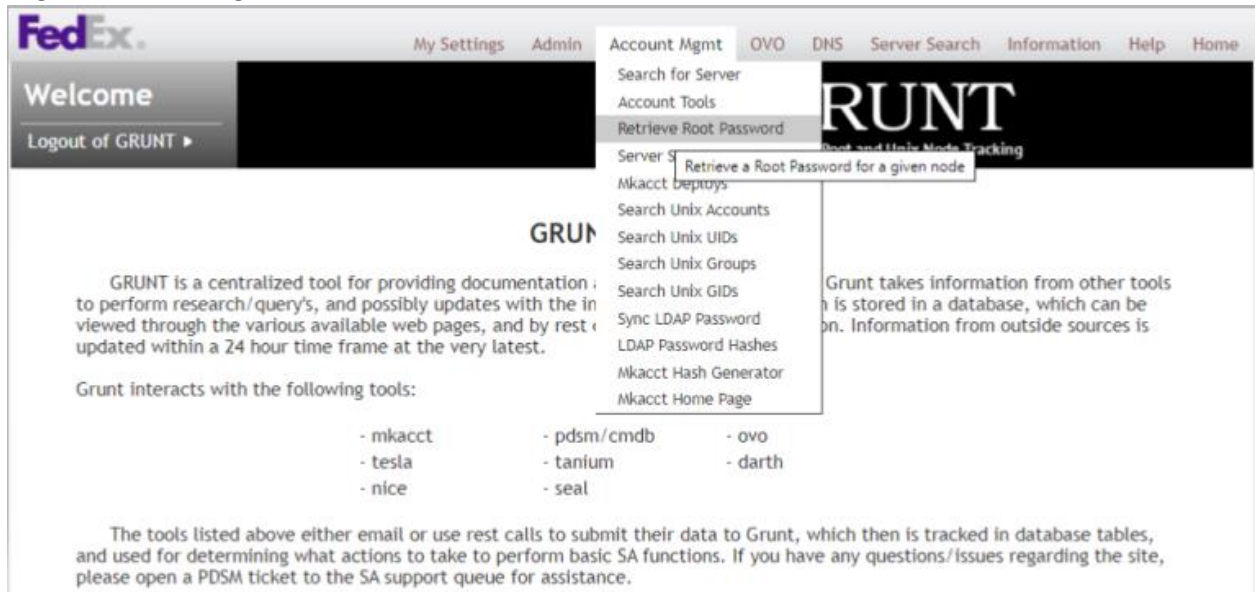
5. If an upgrade is found, select Upgrade
6. Once the upgrade is complete, enter your CORP Username and Password
 - a. Make sure Authentication Type is set to RADIUS



7. On your phone, log into Entrust and locate/enter code into CA token box
Enter a response from your token with serial number

➤ Retrieving root password based on GRUNT information

1. Login into GRUNT, go “Retrieve Root Password” menu:



2. Search for the server to retrieve root password:

Enter Server:

"root" Account is Managed By CAPAM Appliance.

When Logging into CA PAM Client

CA PAM Appliance Address: **pamtest.ute.fedex.com**

After logged into CA PAM Client

Device Name Search: **oss-acctmast.ute.fedex.com**

If you do not have the Client UI yet to access the password through CAPAM, refer to the CAPAM Instructions:

<https://grunt.sac.fedex.com/doc/PamJobAid.pdf>

for the documentation on how to install and use CAPAM client.

If you are in immediate need of the password for an outage, and have issues with the client(including having your CAPAM UI account locked), please email:

pam-oncall-beeper@corp.ds.fedex.com

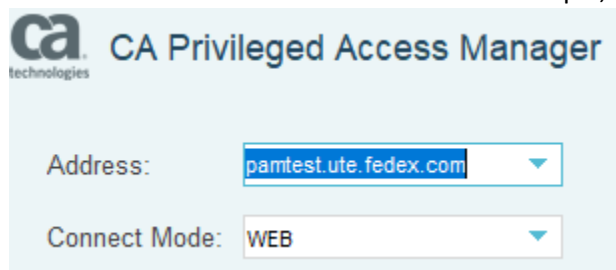
to contact infosec 24/7 support for immediate assistance.

For CAPAM troubleshooting, refer log file to gather more information:

`/var/fedex/mkacct/log/capam.log`

3. GRUNT provides two things:

- CAPAM client address to connect. In this example, we need to connect to “pamtest”.



- After logging into PAM client, search for “Device Name” filter provided by GRUNT

CA technologies CA Privileged Access Manager

Access

Column: Device Name Value: oss-acctmast.ute.fedex.cc FILTER

Device Name	Address	Operating System	Access Methods	Web Port
oss-acctmast.ute.fedex.cc	irh00229.ute.fedex.cc	Linux		

4. To access ‘ROOT’ password:

- Select a server you want to access and click on “SELECT” link under the Target Application icon.

Access

Column: Device Name Value: oss-acctmast.ute.fedex.cc FILTER RESET ADD FILTER MY VIEWS

RESTART SESSION

Device Name	Address	Operating System	Access Methods	Web Portal	RDP Applications	Services	Target Applications
oss-acctmast.ute.fedex.cc	irh00229.ute.fedex.cc	Linux					 SELECT

mkacct_oss-acctmast.ute.fedex.cc

root

- Complete the details for password access in the “Reference code” section. And PAM will show the password of the server.

Access

Column: Device Name Value: ije0070* FILTER RESET ADD FILTER MY VIEWS

Device Name	Address	Operating System
ije00706.ute.fedex.cc	ije00706.ute.fedex.cc	Linux
ije00707.ute.fedex.cc	ije00707.ute.fedex.cc	Linux

Show Password

Reason: Production support

Reason Description:

Reference Code:

Timezone: UTC

OK CANCEL

Access

Column: Device Name Value: ije0070* FILTER

Device Name	Address	Operating	Access Methods
ije00706.ute.fedex.com	ije00706.ute.fedex.com	Linux	SSH
ije00707.ute.fedex.com	ije00707.ute.fedex.com	Linux	SSH

Show Password

Account Name: root

Password: paERTo50

CLOSE

5. Log out of PAM