Table of Contents

Unit 1 Getting Started ......................................................................................................... 5
Hardware and Software Requirements .................................................................................. 5
Who Can Use Privilege Management? .............................................................................. 5
Administrator Roles in Privilege Management ................................................................. 6
Requesting Access ............................................................................................................. 8
Resources in Privilege Management .................................................................................. 8
Resource Groups ............................................................................................................... 9
Resource Group Hierarchies ............................................................................................... 10
Resource Status .................................................................................................................. 12
Inheritance .......................................................................................................................... 13
What is a Privilege Assignment? ......................................................................................... 14
Login ................................................................................................................................. 14
Timeout ............................................................................................................................... 14
Unit 2 Viewing My Privileges ............................................................................................ 15
Purpose .............................................................................................................................. 15
By Privilege View ............................................................................................................... 16
By Resource View ............................................................................................................. 17
Unit 3 The Person Tab ......................................................................................................... 18
Section 1: Viewing Privileges for Someone Else ............................................................... 18
Person Details .................................................................................................................... 19
Section 2: Adding Privileges ............................................................................................. 24
Entering or Searching for a Resource .................................................................................. 24
Add Privilege .................................................................................................................... 28
Submit Privilege ................................................................................................................ 36
Section 3: Editing Privileges ............................................................................................... 37
Section 4: Deleting Privileges ............................................................................................ 39
Section 5: Copying Privileges ............................................................................................. 40
Section 6: Moving Privileges ............................................................................................. 42
  Copying or Moving a Privilege that Already Exists on the Target ..................................... 44
Copying or Moving a Large Number of Assignments................................. 44
Section 7: Suspending and Reinstating Privileges........................................ 45
Managing Leaves of Absence................................................................. 47
Copying and Moving Suspended Privileges.............................................. 47
Unit 4 The Resource Tab ........................................................................ 48
Section 1: Looking up a Resource .......................................................... 48
Section 2: Resource Details by Person .................................................... 50
Drill Up and Drill Down ........................................................................ 52
Section 3: Resource Details by Privilege .................................................. 55
Who can Sign this Form or Approve this Request?................................. 55
Direct and Inherited Privilege Assignments ........................................... 57
Summary: Steps for Determining who Possesses a Particular Privilege on a
Resource.................................................................................................. 59
Unit 5 The My Worklist Tab and Workflow ............................................ 60
Section 1: What is Workflow? ............................................................... 60
What Triggers Workflow in Privilege Management?.............................. 61
Section 2: Entering a Privilege for Workflow ......................................... 63
Section 3: Privilege Reviewer’s and Approver’s Worklist ....................... 64
Approving and Rejecting Pending Privileges ........................................ 65
Approving or Rejecting Multiple Privileges at Once ............................. 67
Section 4: Segregation of Duties and Assigning Privileges .................... 68
Summary: Entering Privileges into Privilege Management..................... 69
Unit 6 The Admin Tab .......................................................................... 70
Section 1: Transfer and Termination Reports ......................................... 70
Transfer Reports.................................................................................... 71
Termination Reports ............................................................................. 73
Section 2: File Upload .......................................................................... 74
Unit 7 Reports Tab .............................................................................. 75
Section 1: Privilege Management Reports in InfoView ......................... 75
Accessing the Reports........................................................................ 75
Navigating to Privilege Management Reports in InfoView ................. 76
Reports.................................................................................................. 79
Unit 6 Help and Logout ......................................................................... 86
Help ........................................................................................................................... 86
Logout ....................................................................................................................... 86
APPENDICES .................................................................................................................. 87
Updates to Privilege Management ................................................................................ 87
  Updates to Resources ............................................................................................... 87
  Changes to Resource Groups .................................................................................. 87
  Updates to Privilege Assignments ........................................................................ 87
Decentralized Administrator Tasks in Privilege Management ......................................... 88
  Monthly Tasks ........................................................................................................ 88
  Annual Task .......................................................................................................... 88
  Tasks to Perform on an As-Needed Basis............................................................... 88
How Copying or Moving Privileges Affects a Privilege Status ....................................... 89
Roles and Access in Privilege Management ................................................................ 90
Privileges, Definitions, and Categories ........................................................................ 90
ePAC Privileges in Privilege Management ................................................................... 91
Glossary of Terms ....................................................................................................... 92
Privilege Management User Guide

Privilege Management is an application used by centralized and decentralized administrators to grant secure access and authorization to Vanderbilt’s information systems and business processes. Access to applications and processes such as eDog, Waldo, Signature Authorization, ePAC, eBudget, DMS, and eProcurement is granted via Privilege Management. In the future, as new systems are developed, they will also be added under Privilege Management’s aegis. Go to the following website to see a list of all Vanderbilt applications administered by Privilege Management:

http://www.vanderbilt.edu/fis/Apps/pm.htm.

Historically, application access had been administered solely by the central financial offices: the Department of Finance, Office of Financial Affairs and Office of Contract and Grant Accounting. Now, designated administrators in the decentralized areas of University Central and VUMC have the ability to administer security for their respective areas. For a concise summary of administrators’ roles and responsibilities, refer to the Privilege Management Policies and Procedures, posted at

http://www.vanderbilt.edu/fis/Apps/pm.htm.

The purpose of this user guide is to provide administrators with the steps to set up and manage user access in the Privilege Management tool. Furthermore, non-administrators can use this guide to learn how to view privilege information in Privilege Management.
Unit 1
Getting Started

Hardware and Software Requirements

Necessary Hardware

Privilege Management is a web-based application and will work on a PC or Macintosh capable of running a supported Internet browser.

Supported Internet Browsers

- Firefox 2.0+
- Internet Explorer 6+ (optimized for versions 7 and above)

Note: Javascript MUST be enabled for Privilege Management to function correctly.

Who Can Use Privilege Management?

Everyone who has one or more active privileges in Privilege Management can log into the application and view privilege information for themselves and others (e.g., I need to find out who in my department can sign my check request form.). Only administrators, however, can manipulate privileges for users within their realm of responsibility, or purview.
**Administrator Roles in Privilege Management**

Top-level administrators are added into Privilege Management via a file upload process, managed in the Financial Information Systems group.

Administrator roles and levels in Privilege Management differ for centralized and decentralized areas in Vanderbilt:

**Centralized**

Centralized areas, where individual departments do **not** manage application access, use the following Administrator Roles:

- **Application Managing Administrators** - set up **administrators** for one specific application, such as eDog or Waldo.
- **Application Administrators** - set up **end users** in one specific application.
  - End users in centralized areas must send access request forms to the Application Administrator for the application to which they need access. Thus, end users needing access to multiple applications must send security request forms to multiple Application Administrators.

```
PM Application Steward
  (Financial Information Systems)
Sets up Application Managing Administrators through a file upload to PM.

Application Managing Administrator
  (Application Specific)
Sets up Application Administrators for a particular application.

Application Administrator
  (Application Specific)
Sets up privileges for departments that don't have security administrators.

End User
  Receives privileges granted by Application Administrator.
```

*Hierarchy for Centralized Security Administration*
Decentralized

Decentralized areas, where individual departments manage application access, use the following Administrator Roles:

- **Decentralized Managing Administrators (DMAs)**- set up Decentralized Administrators, Privilege Reviewers and Privilege Approvers in Privilege Management for their department or area.

- **Decentralized Administrators (DAs)**- grant most non-administrator security assignments for their areas in Privilege Management. DAs administer privileges for multiple applications.

- **Privilege Reviewers**- provide a preliminary approval or rejection of certain high risk roles assigned by DAs. These high risk roles require workflow in Privilege Management, which forces the assignments to go to a higher level for approval before becoming active in Privilege Management and in the requested application. (Not all decentralized organizations use this administrator role in Privilege Management.)

- **Privilege Approvers**- provide final approval or rejection of high risk roles that require workflow and are assigned by DAs.

*Hierarchy for Decentralized Security Administration*
**Requesting Access**

**Administrator Access in Privilege Management**

If you need to be set up as an Application Administrator, Decentralized Managing Administrator, Decentralized Administrator, or Decentralized Administrator Executor, refer to the Privilege Management Application website at [http://www.vanderbilt.edu/fis/Apps/pm.htm](http://www.vanderbilt.edu/fis/Apps/pm.htm) to learn how to request access for the privilege you need.

**Access to Applications Managed by Privilege Management**

To request access to the applications administered by Privilege Management, refer to the consolidated list of application forms and contacts at: [http://www.vanderbilt.edu/fis/Apps/pm.htm](http://www.vanderbilt.edu/fis/Apps/pm.htm).

- If your department is decentralized and has a Decentralized Administrator, send the completed security request form to him/her or email him/her as instructed on the form.
- If your department has no Decentralized Administrator, send the completed security form to the Application Administrator listed on the security form or email the appropriate contact listed.

**Access to Multiple Applications**

If you need access to more than one application, you must fill out a security request form for each application to which you need access.

- If you work in a decentralized department, return all forms to your Decentralized Administrator. He/she will set up all privileges for you, pending approvals.
- If you work in a centralized area, send each form to the appropriate Application Administrator, who is listed on the form. Your privileges will be set up by multiple people, pending approvals.

**Resources in Privilege Management**

**Definition:** A *resource* is a cost center or home department or a group of cost centers or home departments. Privileges are assigned to an individual on a resource.

```
- Human Resources
- Waldo Viewer (Privilege)
  - 4042319856-INGRAM PROG DEV-INFRAS (Resource)
  - 4042330661-5R01CA10216-01-03 (Resource)
```

The example above shows the Waldo Viewer privilege assigned to two resources—cost centers 4042319856 and 4042330661—for a person. Therefore, the owner of this privilege would be able to view Waldo reports for only those two cost centers.
Resource Groups

Cost centers and home departments are organized into logical groupings called resource groups, or *sumtos*. These groupings allow administrators to give access to a lot of centers or home departments in one step when necessary.

**University Central and VUMC Groups**

- **Sumto Center** - An alphanumeric field with six or fewer characters that represents the summary of a group of cost centers.

- **Sumto Home Department** - An alpha field with six characters that represents the summary of a group of home departments.

**VUMC-Only Groups**

- **PCC Sum** - A group of Inpatient, Outpatient and/or Administrative centers strategically servicing patients with similar medical needs or providing support services of a similar nature.

- **PCC Sum Slice** - A subset of a PCC Sum. The PCC Sum Slice is in the Major Operating Division tree and represents a portion of the PCC Names that roll up to a PCC Sum in the PCC Sum tree.

- **Function** - Cost centers grouped in accordance with functional responsibility that generally are performing similar patient care, support or administrative services (e.g., Patient care services, Dietary, General and Administrative, etc.).

- **Major Operating Division** - A high level grouping of cost centers that is typically based on the major operational areas in the Medical Center (e.g., Vanderbilt University Hospital, School of Medicine, School of Nursing).

- **Department** - A group of cost centers that are performing similar administrative, educational, research, and/or healthcare services within a particular field of knowledge or area of specialization. Multiple Departments and/or Sections are grouped to form a Major Operating Division.

- **Division** - A group of cost centers that are performing similar administrative, educational, research, and/or healthcare services within a particular field of knowledge or area of specialization. Multiple Divisions are grouped organizationally to form a Department.

- **Section** - A group of cost centers that are performing similar administrative, educational, research, and/or healthcare services within a particular field of knowledge or area of specialization. Multiple Departments and/or Sections are grouped to form a Major Operating Division.

Centers and home departments can belong to multiple groups, since these resources get grouped in different ways, depending on the need (e.g., cost centers are grouped one way for accounting purposes and another way when reflecting an organizational chart).
When sumto resources are displayed in Privilege Management, the resource type—center, sumto center, home department, sumto home department, division, PCC, MOD, department, or section—is often noted along with the resource name.

**Examples of Resource Groups**

**Sumto Centers and Sumto Home Departments**

![Diagram of Sumto Centers and Sumto Home Departments Example]

**Resource Group Hierarchies**

The table below shows various groupings, or roll-ups, of resources, grouped by functional area at Vanderbilt. Each column begins with the lowest levels of resources and progresses to the highest levels.

**Accounting Hierarchy**

<table>
<thead>
<tr>
<th>All Areas (University and VUMC)</th>
<th>Medical: Patient Care</th>
<th>Medical: Schools &amp; Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Center</td>
<td>Center</td>
<td>Center</td>
</tr>
<tr>
<td>Sumto Center</td>
<td>Sumto Center</td>
<td>Sumto Center</td>
</tr>
<tr>
<td>PCC Sum</td>
<td>Division</td>
<td></td>
</tr>
<tr>
<td>Function</td>
<td>Department</td>
<td></td>
</tr>
<tr>
<td>Major Operating Division</td>
<td>Section</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Major Operating Division</td>
<td></td>
</tr>
</tbody>
</table>

*General Ledger-Based Resources and Roll-ups*
Example: Cost Centers Rolling Up into Resource Groups

The following example shows unrestricted cost centers in the medical school’s pediatrics area rolling up into logical resource groups:

Cost Centers Rolling Up into Resource Groups
**Personnel Hierarchy**

The roll-ups of resources for Human Resources data is the same for all areas:

<table>
<thead>
<tr>
<th>All Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home Department</td>
</tr>
<tr>
<td>(HR data only)</td>
</tr>
<tr>
<td>Sumto Home Department</td>
</tr>
<tr>
<td>(HR data only)</td>
</tr>
</tbody>
</table>

*Personnel-Based Resources and Roll-ups*

**Resource Status**

**Center Status**

A center can have an *open* or *closed* status:

- **Open** - A center that is currently used by departments to record financial transactions.
- **Closed** - A center that is not currently used by departments and has been officially closed in the General Ledger system by the Department of Finance, the Office of Financial Affairs, or the Office of Contract & Grant Accounting. (*Note: All accounts within a center must be closed individually to prevent transactions from posting to the center; however, accounts are occasionally re-opened to permit transactions to post.*)

**Home Department Status**

A home department can have an *active* or *inactive* status:

- **Active** - A home department where personnel are currently assigned and paid.
- **Inactive** - A home department where personnel are no longer assigned and paid.
Inheritance

In Privilege Management, the term *inheritance* refers to having access to a resource by virtue of access to a resource group at a higher level.

If you have a privilege at a sumto center or sumto home department, you automatically have the same assigned privilege on all resources that roll-up to that sumto, even though your VUnet ID is not explicitly assigned to each home department or center.

**Example:** Assume that the following centers belong to the 52410 sumto center for law school loan funds:

Sumto Center 52410

- Employee possesses eDog Viewer privilege at this resource group.

- 5241000012
- 5241000022
- 5241000032
- 5241000052
- 5241000062
- 5241000072
- 5241000082
- 5241000092
- 5241000102
- 5241000112

Employee therefore possesses eDog Viewer privilege on all of the centers that roll-up to the resource group by inheritance.

Inheritance in Privilege Management

---

**Benefit of Making Privilege Assignments to Resource Groups**

A person assigned a privilege at a resource group automatically inherits that privilege for every center or home department rolling up to that resource group. When new centers or home departments are created, they are usually assigned to resource groups. As new centers or home departments get added to a resource group where someone is assigned a privilege, that person automatically inherits the privilege for the newly-added centers or home departments. Therefore, administrators can avoid having to update people’s privilege assignments whenever new centers or home departments are created for their area as long as they’re assigning privileges at resource groups.
What is a Privilege Assignment?

Privilege Management uses three entities to create and manipulate access to applications and signature authority: people, resources, and privileges. A **privilege assignment** is the combination of a privilege for a person on a resource:

![Diagram](image.png)

Login

Access Privilege Management from the eBiz website or the FIS Applications page for Privilege Management:

- **eBiz Website:**
  - From the University home page: [http://www.vanderbilt.edu/ebiz/](http://www.vanderbilt.edu/ebiz/)
  - From the VUMC home page: [http://www.mc.vanderbilt.edu/ebiz/](http://www.mc.vanderbilt.edu/ebiz/)

- **FIS Website:** [http://www.vanderbilt.edu/fis/Apps/pm.htm](http://www.vanderbilt.edu/fis/Apps/pm.htm)

Log in with your VUnet ID and ePassword.

**Timeout**

Your login will automatically time-out after 2 hours of inactivity in the application. No warning message will appear upon timeout.
Unit 2
Viewing My Privileges

Non-administrators in Privilege Management will come to the My Privileges page upon login. If you are a Privilege Management administrator or if you click other tabs in Privilege Management, you can always view your privileges by clicking the My Privileges tab.

Purpose

The purpose of this tab is to show you what privileges have been assigned to you in the Privilege Management application. Using the information provided on the My Privileges tab, you can verify that you have access to applications for the resources you need. Neither end users nor administrators can manipulate (add, edit, delete, copy, move) the privileges displayed on the My Privileges page; the tab is for viewing purposes only.

My Privileges Page - By Privilege View

The top of the My Privileges page shows the following information about you:

- Name
- VUnet ID
- Employee ID
- Employee status
- Home department number
- Home department name
- Job code
- Job code description
By Privilege View

For easier viewing purposes, your assigned privileges first appear grouped by privilege type. Privilege Management categorizes privileges into four types:

- **Financial** - privileges in this category relate to financial applications such as eDog, DMS, and eBudget, and to Signature Authority for financial-related forms.

- **Human Resources** - privileges in this category relate to personnel applications like Waldo and ePAC, and to Signature Authority for personnel-related forms.

- **Privilege Management** (for administrators only) - privileges in this category enable administrators to assign or review/approve other privileges or signature authority to a requestor.

- **Procurement and Disbursements** - privileges in this category relate to eProcurement and to signature authority for Procurement and Disbursements forms like requisitions.

You will only see the privilege types listed for privileges that you possess. For example, if your only roles in Privilege Management are eDog Viewer and Waldo Viewer, you will only see the Financial and Human Resources privilege types listed.

Click the plus sign next to a privilege type to expand it and view the privileges you have in that category. Clicking the plus sign next to the privilege name will show you the resources to which the privilege pertains. (See page 8 for more information on resources.)

Interpreting What you See

The illustration below summarizes the privilege information provided to you in the By Privilege view. Your privileges might differ from the ones displayed here, however. For a complete listing of privileges and their definitions, refer to [http://www.vanderbilt.edu/fis/Documents/PM/All%20Privileges.xls](http://www.vanderbilt.edu/fis/Documents/PM/All%20Privileges.xls).
By Resource View

Clicking the By Resource toggle located above your privilege listing displays your privileges by resource (i.e., by center, sumto center, home department, etc.) instead of by privilege type:

<table>
<thead>
<tr>
<th>Resource</th>
<th>Privilege Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>INGRAM PROG DEV-INFRAS</td>
<td>(Resource)</td>
</tr>
<tr>
<td>4042319856</td>
<td></td>
</tr>
<tr>
<td>Human Resources</td>
<td>(Privilege Type)</td>
</tr>
<tr>
<td>Waldo Viewer</td>
<td>(Privilege)</td>
</tr>
<tr>
<td>Financial</td>
<td>(Privilege Type)</td>
</tr>
<tr>
<td>eDog Viewer</td>
<td>(Privilege)</td>
</tr>
<tr>
<td>4042330661 5R01CA10216-01-03</td>
<td>(Resource)</td>
</tr>
<tr>
<td>Human Resources</td>
<td>(Privilege Type)</td>
</tr>
<tr>
<td>Waldo Viewer</td>
<td>(Privilege)</td>
</tr>
</tbody>
</table>

This view provides you with an easy way to see what privileges you possess for each center (or sumto center, home department, sumto home department, etc.) to which you belong.
Unit 3
The Person Tab

Upon login, Privilege Management administrators will come to the Person tab. This tab is where you begin the process of adding, editing, deleting, copying or moving privileges for employees, students, contractors, etc. in your purview.

Non-administrators who have at least one active privilege in Privilege Management can use this tab to view others’ privileges (e.g., *I need to see if my manager has Signature Authority for my Check Request Form.*). Non-administrators have view-only rights on this tab.

Section 1: Viewing Privileges for Someone Else

Before adding, editing, or deleting privileges for someone, administrators should first view that person’s current privileges and assess the implications of making the requested change: *would adding the requested privilege violate any segregation of duties imposed in your area? Do the resources for the requested privilege make sense based on the other resources and privileges the person possesses?*

Non-administrators can use the person search to determine if their manager or administrative assistant has signature authority for the form in question and for the resource(s) listed on the form.

To look up a person’s privileges

- Click the **Person** Tab.
- Begin typing the person’s name (last, first) or VUnet ID in the Name field.
- Privilege Management will show search results based on what you’ve entered, with the matching text in **bold**. Select your target person by clicking his/her name in the list of results or enter the full name (last, first) or full VUnet ID and select from there.

![Person Search](image)

*Person Search- Results matching “woh”*

The search results first display matches based on VUnet ID, followed by matches on name (last, first) in alphabetical order.
To select your target person, click the name in the list. Privilege Management automatically takes you to his/her Person Details page.

- Note that you **must click your selection from the search** before continuing. Typing in a name or VUnet ID and pressing Enter will result in an error.

**Person Details**

The header information on the Person Details page shows the following information:

- **Name**- name of the person selected.
- **VUnet ID**- VUnet ID for the person selected.
- **Employee ID**- the person’s employee ID number from the HR PeopleSoft system.
- **Home Dept**- the home department number for the selected person.
- **Home Dept Description**- the description of the home department for the selected person.
- **Job Code**- the selected person’s primary job code number from the HR PeopleSoft system; for people with multiple job codes, this field shows the primary job code, which is always an active code.
- **Job Code Description**- the description for the selected person’s primary job code.
**By Resource View**

The default view for Person Details is **By Resource**, meaning the target person’s privileges appear grouped by resource and then by privilege type.

If you are an administrator and if the target person contains privileges in your purview, you will see checkboxes next to the privileges and resources in your purview. Privileges and resources listed without a checkbox indicate privileges the target person contains that are outside your purview. The By Resource view is the only view in which administrators can manipulate privileges in Privilege Management.

### Interpreting Colors

Privilege Management color codes privileges that are in different states:

- **Black**- privilege is **active** in the system. The example above shows that all of the person’s privileges are active.

- **Blue**- privilege is **pending** approval at a higher level before it becomes active. (See page 60 for more information on pending assignments and workflow.)

- **Gray**- privilege is **suspended** and will not become active until it is reinstated. (See page 45 for more information on suspending and reinstating privileges.)

- **Red**- privilege went through workflow and was **rejected** at a higher level of approval. (See page 60 for more information on approving and rejecting privileges in workflow.)

---

*Person Details - By Resource View - Privileges Available for Editing*
By Privileges View

To view data grouped first by privileges and then by resources, click the By Privilege toggle at the top of the list of privileges:

By Privilege

The privileges will appear grouped first by privilege type and then by privilege. The resources to which a privilege belongs appear under the privilege.

Person Details- By Privilege
Determining if the Target Person has a Particular Privilege

Non-administrators can view this information to see if the person they looked up possesses the privilege in question by finding the resource to which the privilege should apply and then determining if the privilege(s) tied to that resource match what they need.

**Example:** I need to know if my manager has the SigAuth Check Request privilege for center 4204509602.

- If you use the **By Resource** view, you can look for center 4204509602 and see if the SigAuth Check Request privilege is listed under the resource:

```
by resource
```

![View SigAuth Check Request Privilege by Resource](image)

The above example shows that the target person does have the SigAuth Check Request privilege for disbursements up to $3,000 for center 4204509602.

- You could also use the **By Privilege** view to look up this information: click **By Privilege**, and expand the Procurement and Disbursements category to show the SigAuth Check Req privilege. Then examine the resources listed under that privilege to see if center 4204509602 is listed.

```
Procurement and Disbursements
```

![View SigAuth Check Request Privilege by Privilege](image)

If either the resource or privilege is not listed, the target person does not possess the privilege.
• **Important**- When assessing whether the target person contains proper authority for signing a form, check the following information:
  - **Resource**- does the center or home department on your form appear as one of the resources for the person you looked up using Person Search?
  - **Privilege**- does the signature authority pertain to the same type of form or transaction for which you need a signature? (E.g., If the person you looked up has only the SigAuth Purchase Req privilege for your center, but you need a Check Request signed, the person does NOT have appropriate signature authority for your form.)

**Interpreting Privileges Assigned to Resource Groups**

When people need privileges for a lot of centers or home departments in the same department or functional area, administrators often assign them to a resource group, such as a sumto center or sumto home department representing their area. (See page 9 for more information on resource groups.)

To determine if a particular center or home department is a part of a resource group listed under someone’s privileges, refer to the Resource Tab section, beginning on page 48, for information on looking up resources in Privilege Management.

If the person you are viewing possesses a lot of resource groups in his/her purview, be sure to check the centers or home departments that belong to the resource groups when looking for particular centers or home departments. It could be that the person does have a privilege on the center or home department you’re looking for, but that center or home department is a part of a resource group.
Section 2: Adding Privileges

Administrators with appropriate access can set users up with new privileges on the Person Details page, under the By Resource view.

To Add One or More Privileges for a Person:

1. Look up the person who will receive the privilege.
2. Click the Add button at the bottom of the screen.
3. Enter the resource(s) to which the privilege(s) will apply.
4. Select the privilege(s) to add, and define any attributes for the privileges, if applicable.

The rest of this section explains in detail how to accomplish the general steps listed above.

Entering or Searching for a Resource

From the By Resources view of the Person Details page, click the Add button at the bottom of the page. Your options for choosing resource(s) appear.

Privilege Management provides two options for selecting resources:
Option 1: Resource Search

This option is the default selection when adding a privilege and mirrors the Person Search functionality. Use it to add privileges for a single resource. It allows you to type in the name of any resource—a low level center, home department or resource group—and choose the resource from a resulting list.

This list only contains resources in your purview.

Search for Resources in Purview Beginning with “15511”

Because multiple resources might match the search criteria you enter, resources are labeled as follows and appear in the order below:

- SumtoHomeDept
- HomeDept
- SumtoCenter- some Sumto Centers have a VUORG label next to the name. See the next page for more information on these resource groups.
- MajorOptDiv (VUMC only)
- Section (VUMC only)
- Dept (VUMC only)
- Division (VUMC only)
- PCCSum (VUMC only)
- PCCName (VUMC only)
- PCCFunction (VUMC only)
- Center

For more information on what each of the preceding resources or resource groups represent, or on assigning privileges to a resource group, refer to page 9.
The VUORG Label

Some resource groups will appear with a VUORG label next to the name. If you want to assign privileges to a group of centers that roll up according to an organizational structure (e.g., Chemistry Department) instead of a fund accounting roll-up (e.g., Medical School Unrestricted), then use resource groups with the VUORG label. For any application that uses centers (instead of home departments), you can assign privileges to either a fund accounting-based roll-up or the organizational-based roll-up of centers.

Click a resource in the search list to select it. Note that you can only select one resource using the Resource Search.

Privilege Management automatically takes you to the next step once you select a resource.
Option 2: Enter Resources

Click this radio button to enter multiple low level cost centers or home departments for which to add privileges. **You cannot enter resource groups using this option.** Type in the centers or home department numbers, separating multiple entries with a space, comma, semi-colon, or hard return. (Adding a space after commas and semi-colons is optional.) You can also copy and paste centers or home departments from an external source, such as an email or spreadsheet containing the resources to which to add privileges.

You can enter a maximum of 100 resources at a time on this screen.

Enter Multiple Cost Centers

Click the Next button to continue to the next step.
Add Privilege

After entering resources, Privilege Management takes you to the Add Privilege screen.

- If you entered resources outside of your purview using the Enter Resources option, Privilege Management will give you an error message at this point.

The resources you entered on the previous screen appear at the top of the page. Review the resources listed to ensure the correct resources are selected. If you find that you need to return to the enter/select resources screen to correct the resources chosen, click the Back button in the lower left area of the screen.

Person Details

Name: Amy C Wohlen  VunetId: wohlen  Employee Id: 0851233  Status: Active

Resources

SumtoCenter - 155110 - ACCOUNTING SERVICES - DIVISION OF ADMINISTRATION SUMMARY - PRICE B

Add Privilege

- Select Privilege Type
- Select Privilege

Add Privileges

The screenshot above shows that the sumto center 155110 was selected from the Resource Search screen. The Resources information also shows the full name of the resource, Accounting Services- Division of Administration Summary, and the responsible person, Price, B.

Show Resource

When you select resource groups to which to add privileges, a Show Resource link appears to the right of the resource group. Click the Show Resource link to view all low-level centers or home departments that roll up to the resource group.

Show Resources for Selected Resource Group
If multiple lower-level resource groups roll up to the selected resource group, only the low level centers and home departments that comprise those groups will appear in the list. Administrators can use this list to confirm that all necessary centers or home departments are included in the selected resource group. Note that a maximum of 2500 resources will appear using this feature, so if you choose to view resources for a resource group containing more than 2500 low level centers or home departments, you will get an error message from the database.

Selecting Privileges

- Click the Add Privilege Type drop-down menu to choose a privilege category. This step makes it easier to select a privilege to enter by filtering out privilege that don’t apply to the category.
  - To select a category, click it from the list.
  - To see what privileges are included in each category, refer to http://www.vanderbilt.edu/fis/Documents/PM/All%20Privileges.xls.
  - If you do not want to filter by categories, choose All from the drop-down list.

- Next, click one or more privileges from the box below. This box contains all the privileges you are able to administer within the selected category for ALL the resources selected. (I.e., if there are privileges in the category that you can administer but not on every resource selected, you will not see those privileges in the list.)

If you chose All instead of a privilege category, the list below will show all privileges that you can administer on all of the selected resources, regardless of category.

Click the privilege you need to enter. To select multiple privileges, hold the control key (Ctrl) while clicking each privilege to enter.

Add Privilege

Procurement and Disbursements

BO Corp Viewer - APPO
eProcurement Reviewer
eProcurement Viewer
SigAuth 1180/SSR

Add

Back

Select Category and Privilege
If you are unsure which privilege to select, use the information icon, 1, to view a definition for a privilege. You must first click a privilege in the list before clicking the information icon and viewing a definition.

Add Privilege

View Definition for Selected Privilege

Click Add.

- Note that Privilege Management does not save this addition to the database at this point. You can continue to add more privileges for the resource(s) selected by choosing another privilege type and privilege before submitting your additions to the database.

- A Target End Date field will appear below the privilege you added.
Target End Date

This information is optional—you are NOT required to enter it before saving the privilege. This field allows you to enter the expected end date through which the person will use the selected privilege. This date is used only for reporting purposes: it does NOT trigger any automatic notifications in Privilege Management.

**Target End Date**

You can use the Target End Date as a reminder to remove someone’s privileges at the correct time.

- **Example:** you have a student worker in your department for one semester who needs eDog access. You can enter a Target End Date for the eDog Viewer privilege that corresponds with the end of the semester. When you run Privilege Management reports including the Target End Date, this privilege will appear as a reminder to remove the privilege for the student.

**To Enter a Target End Date**

- Click in the Target End Date field. A calendar will appear.
- Use the calendar to scroll to the correct month and year.
- Click the date desired; the calendar will close automatically.
- The date you selected will appear in the Target End Date field.

Note that Privilege Management does not enforce any dates entered. Therefore, if you do not modify or delete privileges after their target end dates, the owner of the privilege will continue to have it.

Refer to page 47 for information on setting Target End Dates when suspending privileges for leaves of absence.
To Remove a Target End Date

Click the **Edit** button next to the privilege, click the **Target End Date** field, and click **Clear Date** at the bottom of the calendar. Close the calendar and click Save.

![Clear Target End Date](image.png)

**Using Target End Dates with Privilege Management Reporting**

If you enter Target End Dates for privileges, this information will appear on the Target End Date report from Privilege Management. (Refer to page 75 for more information on Privilege Management reports.) Generate this report routinely (weekly or monthly) to create a list of all privileges that have reached or are approaching their Target End Date. Use this list to guide you in your next steps—either deleting the privileges or adjusting Target End Dates in cases where the privilege owner will need the privilege for a longer duration.
**Attributes**

Some privileges contain *attributes* which give further constraints or description to the access the privilege allows. Examples of attributes include dollar limits, fund types, and federal/non-federal indicators on purchasing or signature authority privileges.

Privileges that have attributes automatically display fields for their attributes once you add the privilege. Use the drop-down arrows to choose the desired setting for each attribute. If you do not make a selection for an attribute, Privilege Management will save the default selection shown.
**Types of Attributes**

Privilege Management provides the attributes listed in the table below. The applications you manage access for in your department will determine which—if any—of the attributes you administer.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Application</th>
<th>Use</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dollar limit</td>
<td>Multiple: eProcurement, SigAuth, ePAC, eBudget</td>
<td>Sets the dollar limits for procurement/disbursements and signature authority privileges.</td>
<td>Select from pre-defined limits or enter your own limit.</td>
</tr>
<tr>
<td>Encumbrance Initiator type</td>
<td>DMS</td>
<td>Determines if the user can use the Budget, Personnel, and/or Non-Personnel tabs in DMS.</td>
<td>Enter Yes or No for each option: Budget, personnel, non-Personnel.</td>
</tr>
<tr>
<td>Type of Distribution PAC</td>
<td>ePAC</td>
<td>Sets limits on PA initiator privilege in ePAC.</td>
<td>All Distrib (EDC, RDC); Earnings distrib changes (EDC); Cost transfer/Retro distrib (RDC)</td>
</tr>
<tr>
<td>Allowed to initiate</td>
<td>ePAC</td>
<td>Sets limits on PA initiator privilege in ePAC.</td>
<td>All PACs; Distrib PACs only</td>
</tr>
<tr>
<td>Distribution PACs</td>
<td>ePAC</td>
<td>Determines if PA Reviewer’s comments are optional or required on distribution PACs.</td>
<td>Optional; required</td>
</tr>
<tr>
<td>Non-distribution PACs</td>
<td>ePAC</td>
<td>Determines if PA Reviewer’s comments are optional or required on non-distribution PACs.</td>
<td>Optional; required</td>
</tr>
<tr>
<td>Federal indicator</td>
<td>eProcurement, SigAuth</td>
<td>When assigning some procurement/disbursements or signature authority privileges at the resource group level, use this attribute to denote if privilege is constrained to only federal or non-federal centers within the group.</td>
<td>Federal; non-federal</td>
</tr>
</tbody>
</table>
### Table continued…

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Applications</th>
<th>Use</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fund type</td>
<td>eProcurement</td>
<td>When assigning some procurement/disbursements or signature authority privileges <strong>at the resource group level</strong>, use this attribute to denote if privilege is constrained to only restricted or unrestricted centers within the group.</td>
<td>Restricted; unrestricted</td>
</tr>
<tr>
<td>Allowed to approve</td>
<td>SigAuth (for PAFs)</td>
<td>Constrains the types of forms the privilege owner is allowed to sign.</td>
<td>EDC and RDC PACs only; PayRate, StdHrs, EDC, RDC PACs</td>
</tr>
</tbody>
</table>

**Dollar Limit Attributes**

When adding or editing a dollar limit attribute, the drop-down menu contains an option for an amount other than those provided. If you select *Other* from the drop-down menu, you must type the dollar limit in the field that appears to the right. Enter whole numbers without commas, decimals, or dollar signs.

**Add Privilege**

![Add Privilege](image)

**Enter a user-defined dollar limit as a whole number, without a comma, decimal, or dollar sign.**

**Entering an “Other” Dollar Limit for an Attribute**

![Entering an “Other” Dollar Limit for an Attribute](image)
The amount you enter in the user-defined field is **inclusive** of (less than or equal to) the dollar limit. In the preceding example, the eProcurement Executor privilege has a limit of $1,500, meaning any eProcurement transaction **over** $1,500 would exceed the privilege owner’s authority.

**Submit Privilege**

When you’ve finished entering all the privileges necessary for the resource(s) selected, click the **Submit** button at the bottom of the screen. At this point, Privilege Management saves all the privilege assignments added and displays all privileges for the selected person.

Once you submit privileges in Privilege Management, they either become active immediately or go into a pending state, which requires approval from someone higher in the organization before becoming active. Active privileges appear in black on a Person Details page; pending privileges appear in blue. (See page 60 for more information on pending assignments and workflow.)

Once a privilege is active, the person receiving the privilege can log into the application he/she received access to and use it for the resource(s) included with the privilege.

**Application Privileges Not Limited by Resource**

This information only applies to Decentralized Managing Administrators (DMAs). When Decentralized Managing Administrators (DMAs) assign the Decentralized Administrator (DA) privilege on resources, the privilege will appear under two sections on the Person Details page: 1.) under the resource selected when adding the privilege and 2.) under a heading labeled “Application Privileges Not Limited by Resource.” This entry automatically gets included with the DA privilege to allow the DA to assign eProcurement privileges. If a DMA deletes, copies, or moves a DA privilege assignment, the Application Privileges Not Limited by Resource entry will automatically get deleted/copied/moved too. This label does not appear with a checkbox since it automatically gets deleted, copied, and moved. Because this label is technically not a resource, it does not appear under the Resource tab. (See page 48 for more information on the Resource tab.)

**Adding a Privilege that Already Exists**

If you add a privilege for someone, and that person already possesses that privilege on the same resource(s), the new entry will **overwrite** the existing one. You will not receive a warning in this case.

**Duplicate Privileges with Attributes**

If you enter a privilege with attributes where the person, resource(s), and privilege(s) are identical but the attributes differ, the new privilege will **overwrite** the previous one.
Privilege Management cannot distinguish between like privileges on the same resource(s) when only their attributes differ.

- **Example:** if an employee already has eProcurement Reviewer for $1,000 on a center, and you enter the eProcurement Reviewer privilege for $5,000 on the same center, the new privilege with the $5,000 limit will overwrite the original privilege with the $1,000 limit.

### Section 3: Editing Privileges

In addition to adding new privileges, administrators can edit existing privileges to add or change the Target End Date or to edit attributes.

**You must be in the default view, by Resource, to make any changes to a person’s privileges.**

To edit a privilege, click the Person tab and select the person for whom you will edit a privilege.

In the by Resource view, privileges that fall within your purview appear with a checkbox and Edit button next to them.
Click the **Edit** button next to the privilege you want to edit. At this point, the information available for editing appears in bold text:

```
[ ] Procurement and Disbursements
  [ ] SigAuth Check Req
  [ ] Target End Date: [ ]
  [ ] Dollar Limit: < $25,000

Save  Cancel
```

*Editing a Privilege*

In the example above, we’ve edited the SigAuth Check Request privilege and reduced the Dollar Limit attribute from unlimited to $25,000.

Click the **Save** button to save the changes, or click **Cancel** to revert to the original privilege settings. At this point, the bold font disappears; the Target End Date field also disappears if you did not add a date. (Refer to page 31 for information on Target End Dates and how to enter/change them.)

```
[ ] Procurement and Disbursements
  [ ] SigAuth Check Req
  [ ] Dollar Limit: < $25,000
```

*Edited Privilege Saved*

Note that if you are a Decentralized Administrator and you edited a privilege that requires workflow, the privilege will appear in **blue** instead of black. (See page 60 for more information on workflow.)
Section 4: Deleting Privileges

Like adding and editing privileges, administrators can delete privileges within their purview.

To delete a privilege, click the Person tab and select the person for whom you will remove a privilege.

In the by Resource view, privileges that fall within your purview appear with a checkbox next to them. Click the checkbox next to any privilege you want to delete and click the Delete button at the bottom of the screen.

Note that no warning message appears before Privilege Management executes the deletion, so be sure you’ve selected the correct privileges before clicking Delete.
Section 5: Copying Privileges

Administrators can copy privileges from one person to another to assign duplicate privileges to another person.

To copy a privilege, click the Person tab and select the person possessing the privilege(s) you want to copy.

In the by Resource view, privileges that fall within your purview appear with a checkbox next to them. Click the checkbox next to any privilege you want to copy to someone else and click the Copy button at the bottom of the screen.

View by resource

Check the box next to all privileges to be copied.

To select and copy all privileges for a resource, check the box next to the name of the resource.
After clicking the Copy button, the Copy Assignments dialog box appears:

In the Name field, enter the last name or VUnet ID of the target person who will receive the duplicate privileges. The name field functions like the name field on the Person page. (See page 18 for more information on Person Search.)

Under Assignments, verify that the privileges listed are the correct privileges to copy. If so, click **Submit**. If not, click **Cancel** and return to the source person’s details page to re-select privileges for copying.

When you click Submit, the target person’s details page appears showing all of his/her privileges, including the newly-copied ones.

Copying privileges duplicates all privilege information, including attributes and Target End Dates.
Section 6: Moving Privileges

Administrators can move privileges, which removes the privileges from the original person and adds them to the second person.

To move a privilege, click the Person tab and select the person possessing the privilege(s) you want to move.

In the by Resource view, privileges that fall within your purview appear with a checkbox next to them. Click the checkbox next to any privilege you want to move to someone else and click the Move button at the bottom of the screen.

Check the box next to all privileges to be moved.

To select and move all privileges for a resource, check the box next to the name of the resource.

Person Details - Select Privileges for Moving
After clicking the Move button, the Move Assignments dialog box appears:

![Move Assignments Dialog Box]

**Move Assignments**

In the Name field, enter the last name or VUnet ID of the target person who will receive the privileges. The name field functions like the name field on the Person page. (See page 18 for more information on Person Search.)

Under Assignments, verify that the privileges listed are the correct privileges to move. If so, click **Submit**. If not, click **Cancel** and return to the source person’s details page to re-select privileges for moving.

When you click Submit, the target person’s details page appears, showing all of his/her privileges, including the newly-moved ones.

![New Privileges on Target Person’s Details Page]

**New Privileges on Target Person’s Details Page**

Moving privileges moves all privilege information, including, attributes and Target End Dates. Because these privileges were moved instead of copied, the source person no longer possesses these privileges.
Copying or Moving a Privilege that Already Exists on the Target

If you copy or move a privilege to someone and that person already possesses that privilege, the new entry will overwrite the existing one. You will not receive a warning in this case.

Copying or Moving a Large Number of Assignments

If you copy or move a large number of privilege assignments, your browser might time out before the database server finishes processing the copy or move. In this case, you will receive a message in Privilege Management informing you of the occurrence; however, the copy or move WILL complete.

To view the copied or moved privileges, you will have to use the Person tab to access the target person’s details page. If you do not see all of the privileges you expect to see on the Person Details page, it is because some of the privileges are still being copied or moved. Wait a few minutes and recheck the page for updates.
Section 7: Suspending and Reinstating Privileges

Administrators can suspend privileges, which maintains the privilege assignment in Privilege Management, but makes the privilege inactive so the privilege owner cannot access the relevant application. Administrators can use this functionality to maintain security for leaves of absence without deleting and re-adding the privileges once the owner returns from leave.

To suspend a privilege, click the Person tab and select the person for whom you will suspend privileges.

In the by Resource view, privileges that fall within your purview appear with a checkbox next to them. Click the checkbox next to any privilege you want to suspend and click the Suspend button at the bottom of the screen.

Person Details - Select Privileges to Suspend
Once you click the Suspend button, the suspended privileges appear in gray and will continue to do so until the privileges are reinstated, or reactivated. The owner of the suspended privileges will no longer have access to the related applications or signature authority for the related transactions until you or another administrator reinstates the privileges.

**Reinstating Suspended Privileges**

To reinstate suspended privileges, click the Person tab and select the person for whom you will reinstate privileges.

In the by Resource view, privileges that fall within your purview appear with a checkbox next to them. The suspended privileges appear in gray. Click the checkbox next to any suspended privilege you want to reinstate and click the **Reinstate** button at the bottom of the screen. Once you click the Reinstate button, the privileges will again appear in black, as active privileges. The privilege owner will be able to log into the related application and use it at that point.
Managing Leaves of Absence

If an employee in your department will be taking a leave of absence for a length of time you deem necessary for suspending privileges, first copy that employee’s privileges to the person or persons who will assume those responsibilities during the leave of absence. (See page 40 for details on copying privileges.) Then suspend the privileges for the original employee. You can add a Target End Date to the suspended privileges to remind you to reinstate these privileges upon the employee’s return.

When that employee returns from the leave of absence, reinstate his/her privileges and remove or adjust the copied privileges for the backup-employee(s) as needed.

Copying and Moving Suspended Privileges

If you suspend privileges before copying or moving them, the copied privileges will also be in a suspended state for the target person. Follow the procedures above to reinstate a copied, suspended privilege.
Unit 4
The Resource Tab

All Privilege Management users have access to the Resource tab in the application. This tab allows you to look up information for any resource included in Privilege Management—any center, home department, sumto center, sumto home department, MOD, PCC, etc. The resources you can view on this tab are not bound by your purview (for administrators) or the resources for which you have application access.

Administrators use the Resource tab to view consolidated information about the resources for which they are responsible.

- Examples: I want to see all privileges assigned on resources in my purview; or I want to see everyone who is an eProcurement Executor on a particular resource I manage.

Administrators cannot add or manipulate privileges displayed on the Resource tab, but information from this tab can assist admins in assigning privileges on the Person tab.

Non-administrators can use this tab to look up others’ privileges on their centers.

- Example: I want to see who has the SigAuth Travel privilege on my center to be sure I have the correct person sign my travel expense form.

Section 1: Looking up a Resource

To find a resource on the Resource tab, type the name or number in the Resource Name or Description field. Like Person Search, you can enter partial text, and Privilege Management will return all matches containing the text you enter.
Because multiple resources might match the search criteria you enter, resources are labeled as follows and appear in the order below:

- SumtoHomeDept
- HomeDept
- SumtoCenter- some Sumto Centers have a VUORG label next to the name. See the next page for more information on these resource groups.
- MajorOptDiv (VUMC only)
- Section (VUMC only)
- Dept (VUMC only)
- Division (VUMC only)
- PCCSum (VUMC only)
- PCCName (VUMC only)
- PCCFunction (VUMC only)
- Center

For more information on what each of the preceding resources or resource groups represent, refer to page 9.

To select a resource, click it in the list. The Resource Details page will appear.
Section 2: Resource Details by Person

Header information for the Resource Details page shows the name and description of the resource, along with the type of resource (center, home department, sumto center, PCC, etc.). Centers, sumto centers, home departments and sumto home departments also show the responsible person. For center-based resources, the responsible person refers to the Center Responsible Person (CRP) from the General Ledger. For home department-based resources, the responsible person refers to the PAF Responsible Person from PeopleSoft.

The default view of the Resource Details screen is by Person, meaning privilege information for the resource will be grouped by the names assigned privileges on that resource or on a resource group that contains the selected resource.

Assignee names are initially collapsed.

- To view privilege information for a person, click the plus sign next to his/her name.
- To view privilege information for all names assigned to the resource, click the expand all link directly above the list of names. Click the collapse all link to revert to the default, collapsed view.
- To view all privilege information for a particular person, click his/her name. This will take you to the Person Details page for the chosen person and show all of his/her assignments on all resources. (See page 19 for more information on Person Details.)

Resource Details

Resource PED1
Resource Description PEDIATRICS UNRESTRICT
Resource Type SumtoCenter
Responsible Person ALTEMIEIER

Click a name to view the Person Details page for that person.

Click the expand all link to view privilege assignments for all names listed.

Click the plus sign next to a name to view all direct and inherited assignments that person has on the selected resource.

Resource Details- by Person View for Resource PED1
When you expand a name, assignments are grouped by whether they are direct or inherited.

In the example above, William D. Bailey is assigned the Decentralized Admin privilege directly at the PED1 resource. By inheritance, William D. Bailey is also able to sign certain PAFs and set up Waldo users for PED1, because the SigAuth PAF and Waldo Administrator assignments are at resource groups containing the PED1 sumto center.

To view the Resource Details page for one of the higher-level resource groups that provide William D. Bailey with inherited SigAuth or Waldo privileges for PED1, click the corresponding link. In the above example, clicking the VANDERBILT UNIVERSITY resource group would access its Resource Details page.
Drill Up and Drill Down

To see to what higher-level resource group(s) the selected resource rolls up, click the **Drill Up** button at the top of the page. The resource group(s) displayed show the next level up in the hierarchy in which the resource rolls up. If multiple resources are listed in the Drill Up window, it indicates that the resource rolls up in multiple hierarchies.

To see what resources or resource groups roll-up to the resource for which you’re viewing details, click the **Drill Down** button. Drilling down takes you one level down in the hierarchy, so if resources roll up multiple times before forming the resource group you’re viewing, drilling down will only show you the roll-up that immediately precedes the selected resource group. If your selected resource is in multiple hierarchies, you might see multiple resources or resource groups listed in the Drill Down window.

### Resource Details

**Resource** PED1  
**Resource Description** PEDIATRICS UNRESTRICT  
**Resource Type** SumtoCenter  
**Responsible Person** ALTEMEIER

Drill Up and Drill Down Buttons on Resource Details Page

**Drilling Up**

Drilling Up from the PED1 resource shows the next-highest-level resource group(s) to which PED1 rolls-up. Clicking a resource listed takes you to the Resource Details page for that resource.

<table>
<thead>
<tr>
<th>Resources this resource rolls up to</th>
</tr>
</thead>
<tbody>
<tr>
<td>SumtoCenter - CLIN1 - MED SCH CLINICAL UNRES - CARMICHEL</td>
</tr>
</tbody>
</table>

Resource to which PED1 Rolls-Up

The screenshot above shows that PED1 rolls up to the CLN1 resource group which represents certain medical school clinics.
Drilling Down

Drilling down from the PED1 resource group shows multiple resource groups that reside one level below PED1 in one or more hierarchies of centers and sumto centers for the medical center.

How to use this information:

When administrators are making assignments at many low-level centers or home departments (and in some cases, at resource groups) they can use the Drill Up information to determine if the assignments should be placed at a higher-level resource group instead of many low-level resources. Administrators benefit from assigning people at resource groups instead of many low-level centers or home departments because it saves time in making assignments and prevents additional assignments when new centers or home departments are added to a resource group.

Likewise, administrators can use the drill up and drill down features to examine how their centers or home departments are grouped into various hierarchies in their area. Knowing these hierarchies makes privilege assignment faster and more efficient for administrators when they know the best resource to which to assign privileges.
Summary: Drilling Up and Drilling Down for Sumto PED1

Drilling up or down on the Resource Details page always takes you one level above or below (respectively) the selected resource.
Section 3: Resource Details by Privilege

Who can Sign this Form or Approve this Request?

The Resource Details-by privilege view shows you who has a particular privilege for a particular resource (e.g., *Who can sign my check request form for my center?*) To view resource details organized by privileges instead of by person, click the **by privilege** link. The initial layout is collapsed, with only privilege categories displayed.

To view all privileges belonging to a category, click the plus sign next to that category. To view all privilege assignments for all categories, click the **expand all** link.
All privilege categories, privileges, and assignee names shown in this view will be for the selected resource only.

View by privilege.

Click the plus sign next to a category to view the privileges from that category assigned on the selected resource.

Click the plus sign next to a privilege to view the names of people assigned that privilege on the selected resource. Names are grouped by whether they are directly assigned to the resource or have the privilege by inheritance. As this example shows, some privileges have attributes that you must also expand before seeing privilege assignments.

Resource Details for PED1 by Privilege- Procurement and Disbursements Category Expanded

Note that only privilege categories and privileges that are assigned on the selected resource appear in this view. Therefore, not all privilege categories or privileges will appear for every resource.
Direct and Inherited Privilege Assignments

For a particular privilege, assignments are shown based on whether they are direct or inherited from a higher-level assignment. Expanding the Direct or Inherited links shows the names of the people assigned that privilege for the selected resource. The absence of either the Direct or Inherited link under a privilege indicates that there are no direct or inherited assignments respectively for that resource. If a particular privilege does not appear under a resource, it indicates that there are no such privilege assignments, even inherited ones, for that resource.

- Note: When viewing resources by privilege, you might see a person’s name repeated under a privilege’s Inherited node. This indicates that that person possesses the selected privilege by inheritance from multiple assignments. For example, if you were assigned the eDog Viewer privilege on two sumto centers for your department, in the Resources by privilege view, your name would appear twice under a cost center that rolls up to both sumto centers. The sumto center at which you were directly assigned the eDog Viewer privilege would appear next to its corresponding entry for clarification.

The example on the next page shows the person directly assigned the SigAuth Check Request privilege with the <$25,000 attribute for the PED1 resource. In this example, there are no inherited assignments for this privilege and attribute for PED1.

Clicking an assignee’s name takes you to the Person Details page for that person. (See page 19 for more information on Person Details.)
For privileges with attributes, expand an attribute to see people assigned at that attribute level.

For the selected privilege, expand the Direct or Inherited node to see everyone assigned that privilege for the resource.

Click a name to go to the Person Details page for that person and view all of his/her privilege assignments.

Viewing Names Assigned to Selected Privilege

The above example shows that Thomas Head has the SigAuth Check Request privilege for up to $25,000 for the PED1 sumto center. Therefore, Thomas also has this privilege on any cost center or sumto center that rolls up to PED1. If we had a check request for a value under $25,000 for one or more centers that roll up to PED1, then Thomas Head should sign the check request form.

Note that administrators cannot manipulate privileges directly from either view on the Resource Details page; they must go to the Person Details page to manipulate privileges.
Summary: Steps for Determining who Possesses a Particular Privilege on a Resource

1. In Privilege Management, click the Resource tab.

2. Type in the name or number of the resource in question. To select the resource, click it from the dynamic list that appears.


4. The Resource Details page will refresh, this time organized by privilege categories.

5. Expand the privilege category that contains the privilege in question by clicking the plus sign next to the category name. (Refer to page 16 for descriptions of the types of privileges contained in each category.) You can also click the expand all link to see all privileges and assignments for all categories; however, this could produce a long list, depending on the resource and its assignments.

6. If you did not click the expand all option, next expand the privilege in question by clicking the plus sign next to the privilege name.

7. Expand the Direct and/or Inherited nodes to view all names assigned to them. Anyone assigned to either the Direct or Inherited node for the privilege will have the permission to authorize or execute the related function.

**TIP:** When looking up privileges with dollar limits, choose the dollar limit attribute that most closely matches your needs, inclusive of the dollar amount on your form or purchase.

- E.g., if you have a check request form for $625, choose the lowest dollar attribute listed that exceeds $600. In this example, if you saw attributes of $500, $1,000 and $5,000, choose the $1,000 option because it accommodates your $625 check request but does not go to a higher level than necessary for approval.
Unit 5
The My Worklist Tab and Workflow

Privilege Management administrators, including reviewers and approvers, will see more tabs across the top of the application than non-administrators will. These tabs offer features only administrators will need within the application. Features such as reporting and managing privileges requiring workflow appear under these tabs.

The My Worklist tab applies to Decentralized Administrators, Privilege Reviewers and Privilege Approvers who handle privileges requiring workflow. For more information on the roles of Decentralized Administrators, Privilege Reviewers or Privilege Approvers, refer to page 7.

Section 1: What is Workflow?

Workflow is a process in Privilege Management where high-risk privilege assignments automatically go to a Privilege Approver (and sometimes to a Privilege Reviewer beforehand) for approval before becoming active. The requested privilege remains in a pending state and appears in blue from the time the Decentralized Administrator enters it until it is either approved or rejected by the Privilege Approver. If approved, the privilege becomes active immediately. If the Privilege Reviewer or Approver rejects the requested privilege, he/she must provide a comment explaining the denial. The rejected request and its comment return automatically to the Decentralized Administrator’s worklist for review. From there, the Decentralized Administrator can delete the request if no further action should be taken, or the Decentralized Administrator can edit the request and re-submit it for approval.

Workflow in Organization without Reviewer Level of Approval

Workflow in Organization with Reviewer Level of Approval
What Triggers Workflow in Privilege Management?

The combination of the following conditions invokes workflow:

- Adding, copying, moving, or editing a privilege that is workflow-eligible (see Table 5-1 below). Note that editing attributes and Target End Dates also invokes workflow.
- A Privilege Reviewer and/or Approver in the same department or division at a level higher than the Decentralized Administrator.

When a Decentralized Administrator submits privileges under the above conditions, the privilege automatically assumes a pending status instead of an active status.

If a Decentralized Administrator submits a privilege listed in Table 5-1 but no Privilege Reviewer or Approver exists in the organization, workflow will not be invoked; the privilege will become active immediately. Likewise, if a Decentralized Administrator submits a privilege not listed in Table 5-1, the privilege will become active immediately, regardless of whether or not a Privilege Reviewer/Approver exists in the organization.

Privileges Eligible for Workflow

When a Privilege Reviewer or Approver exists in an organization, the following privileges will automatically go to him/her for approval or denial before becoming active in Privilege Management:

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Budget Approver</td>
<td>Enables holder to review, add cost center comments, approve or reject budgets in the eBudget web application.</td>
</tr>
<tr>
<td>eDog Transaction Approver</td>
<td>Enables holder to certify the completion of the monthly reconciliation of transaction data by report period/fiscal year within eDog.</td>
</tr>
<tr>
<td>Encumbrance Dept Admin</td>
<td>In the DMS web application, this privilege has the capability to create/edit budgets, non-personnel encumbrances, personnel encumbrances, planned budgets and encumbrances. In the Privilege Management web application, this privilege has the capability to add, delete or change the Encumbrance Initiator and Encumbrance Viewer privileges. * Please limit this privilege to 2-3 persons per department.</td>
</tr>
<tr>
<td>eProcurement Executor</td>
<td>Enables holder to approve or reject eProcurement requisitions in eProcurement application.</td>
</tr>
<tr>
<td>PA HD Executor</td>
<td>Enables holder to update, approve or reject Personnel Action Changes in ePAC web application. Review serves as the final level of departmental approval.</td>
</tr>
<tr>
<td>SigAuth Check Request</td>
<td>Enables holder to approve financial transactions processed through Check Request Forms (paper form), which enables him/her to order supplies from stock.</td>
</tr>
<tr>
<td>SigAuth Addl Pay</td>
<td>Enables holder to approve financial transactions processed through Additional Pay Forms (paper form). This process enables the payment of an additional salary distribution to a particular employee.</td>
</tr>
<tr>
<td>SigAuth Approver</td>
<td>Enables holder to approve changes to SigAuth privileges. (University Central only)</td>
</tr>
<tr>
<td>SigAuth BO Security</td>
<td>Enables holder to authorize changes to BO Security. (University Central only)</td>
</tr>
<tr>
<td>Privilege Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SigAuth Budget</td>
<td>Enables holder to approve new or revised budgets. (Medical Center only)</td>
</tr>
<tr>
<td>SigAuth Capital Req</td>
<td>Enables holder to approve financial transactions processed through capital equipment purchase requisitions (paper form).</td>
</tr>
<tr>
<td>SigAuth Check Req</td>
<td>Enables holder to approve financial transactions processed through Check Requests (paper form). This process is used for refunds, reimbursements, and payments for services other than consulting projects totaling $5,000 or more.</td>
</tr>
<tr>
<td>SigAuth Check Travel Ad/Exp</td>
<td>Enables holder to approve financial transactions processed through Travel Advance and Expense Forms (paper forms). This process is used for the advance payment or reimbursement of expenses for travel outside the Metro area.</td>
</tr>
<tr>
<td>SigAuth eDog Security</td>
<td>Enables holder to authorize changes to eDog Security. (University Central only)</td>
</tr>
<tr>
<td>SigAuth PAF</td>
<td>Enables holder to approve financial transactions processed through Personnel Action Changes (paper form or ePAC), Payroll Check Distribution Authorization Forms (paper form), and Home Department Change Forms (paper form), which establish pay rate and job codes for employees. In addition, holder serves as final approval for Pay Rate Standard Hour Earnings Distribution and Retroactive Distribution PACs in the ePAC web application.</td>
</tr>
<tr>
<td>SigAuth PRQ/PMF</td>
<td>Enables holder to approve Position Management Forms (formerly PRQ), which are used for adding or changing employment positions.</td>
</tr>
<tr>
<td>SigAuth Purchase Req</td>
<td>Enables holder to approve financial transactions processed through Purchase Requisitions (paper form).</td>
</tr>
<tr>
<td>SigAuth Reclass/PDQ</td>
<td>Enables holder to approve the financial transactions processed through Reclassification questionnaires (paper form). The questionnaire compiles information required to reclassify an existing or new position (e.g., salary range, pay grade, etc.).</td>
</tr>
<tr>
<td>SigAuth Small PO</td>
<td>Enables holder to approve financial transactions processed through Small Purchase Orders (paper form). These transactions cannot exceed $500.</td>
</tr>
<tr>
<td>SigAuth Stipend Req</td>
<td>Enables holder to approve the financial transactions processed through Stipend Request Forms (paper form).</td>
</tr>
<tr>
<td>SigAuth Timesheet</td>
<td>Enables holder to approve the financial transactions processed through timesheets (paper form or Kronos time records).</td>
</tr>
<tr>
<td>SigAuth Travel Auth</td>
<td>Enables holder to approve financial transactions processed through Travel Authorizations (paper form). This form is used by an employee to request travel.</td>
</tr>
<tr>
<td>SigAuth WALDO Security</td>
<td>Enables holder to authorize changes to WALDO Security. (University Central only)</td>
</tr>
</tbody>
</table>

*Table 5-1: Privileges Eligible for Workflow*
Section 2: Entering a Privilege for Workflow

When a Decentralized Administrator adds, copies, moves, or edits attributes or Target End Dates for any privilege included in Table 5-1 and a Privilege Reviewer and/or Approver exists for the organization, the privilege will go into a pending state and appear in blue on the Person Details page (see page 19 for more information on the Person Details page):

At this point, the pending privilege also appears on the Privilege Reviewer’s worklist. In organizations without a Privilege Reviewer, the pending privilege goes directly to the Approver’s worklist.
Section 3: Privilege Reviewer’s and Approver’s Worklist

My Worklist

Pending Worklist Items for Privilege Approver

The following information appears on the Privilege Reviewer’s and Approver’s worklists:

- **Employee Name** - the name of the person receiving the pending privilege.
  - Mousing-over an employee name shows the job code and job description for that person.

![Employee Name Example](Image)

- **Privilege** - the name of the privilege proposed for the employee.
- **Resource** - the name of the center, home department, or resource group to which the privilege will apply for the employee.
- **Submitted** - the VUnet ID of the Decentralized Administrator who entered the pending privilege assignment.
  - Mousing-over the VUnet ID shows the first and last name of the Decentralized Administrator who initiated the workflow process.

![Submitted Example](Image)

- **Modified Date** - the date and timestamp of when the Decentralized Administrator submitted the pending privilege.
• **Status**- the state of the privilege. Privilege Reviewer’s and Approvers’ worklist items always show a status of *pending*. Privileges on Decentralized Administrators’ worklists contain statuses of *pending* or *rejected*.

• **Show/Hide Inherited Items**- toggle at the top of the worklist allowing the following:
  - **Show Inherited Items**- if clicked, the worklist shows all pending privilege assignments on resources belonging to the Privilege Approver through inheritance in addition to pending privileges on resources where the Privilege Reviewer/Approver is directly assigned.
  - **Hide Inherited Items**- if clicked, the worklist shows only pending privilege assignments on resources where the Privilege Reviewer/Approver is directly assigned.
  - See page 13 for more information on inheritance.

When Privilege Reviewers/Approvers log into Privilege Management, their My Worklist page automatically appears if their worklist contains pending assignments. If the worklist contains no pending assignments, Privilege Reviewers/Approvers see the Person page upon login.

### Approving and Rejecting Pending Privileges

Privilege Reviewers and Approvers should review pending privilege assignments and determine if they are appropriate. When reviewing pending privileges, consider the following criteria:

• Does the privilege make sense, based on the employee’s job duties?

• Is the resource where the privilege is assigned appropriate?
  - For pending privileges on multiple resources: should the assignment be at a resource group instead?

• Would adding the proposed privilege violate any segregation of duties? (See page 68 for more information on segregation of duties.)

• For privileges involving dollar limits, are the dollar limits appropriate, considering the employee’s job duties and dollar limits on his/her other privileges?

To view more detailed information about the employee’s current and pending privileges, click the employee’s name in the worklist:

![My Worklist](image)

*Accessing the Person Details Page from the Worklist*
The employee’s person details page appears.

After reviewing the privilege request, determine whether to approve or reject it. Privilege Reviewers and Approvers will see Approve and Reject buttons at the bottom of the Person Details page and at the bottom of their worklist.

**Approving a Request**

To approve a request, click its checkbox and click the Approve button.

- For Privilege Reviewers, the approved privilege—which is still pending—moves off their worklist and appears as pending in the Privilege Approver’s worklist.
- For Privilege Approvers, the approved privilege disappears from the worklist and appears as an active privilege (in black) on the Person Details page.
Rejecting a Request

The steps for rejecting a request are identical for Reviewers and Approvers. To reject a request, click its checkbox and click the **Reject** button. **You must provide a comment explaining why you’ve rejected the request** so the Decentralized Administrator will know what further steps to take (e.g., *reduce the dollar limit on the privilege* or *assign the privilege to someone else*). Click **Submit** to save the rejection, or click **Cancel** to revert the privilege back to its pending status.

![Comments](image)

**Enter Comment for Rejected Privilege Request**

Rejected requests disappear from the Privilege Reviewer’s or Approver’s worklist and appear on the Decentralized Administrator’s worklist. Rejected requests also appear on the Person Details page in a rejected status (red). A rejected request will remain on the Person Details page and on the Decentralized Administrator’s worklist until the Decentralized Administrator edits and resubmits it or deletes it.

![Rejected Privilege Request in Decentralized Administrator’s Worklist](image)

**Rejected Privilege Request in Decentralized Administrator’s Worklist**

The comment provided by the Reviewer or Approver appears in the note icon to the right of the word **Rejected** on the worklist. Click the icon to view the comment. Note that this comment does not appear with the rejected request on the Person Details page.

**Approving or Rejecting Multiple Privileges at Once**

To approve or reject multiple privileges at once, click all the appropriate checkboxes, or use the Select All button to select all pending privileges on the page. Then click the Approve or Reject button.

If you select multiple privileges and reject them, only one comment box will appear. Be sure to provide feedback on all privileges you rejected.
Section 4: Segregation of Duties and Assigning Privileges

Segregation of duties refers to the concept that, ideally, the same person should not be responsible for the acquisition of goods or services, the approval of that acquisition and the reporting/record keeping of the transaction. Such a combination of responsibilities can increase Vanderbilt’s risk for fraud or other financial impropriety. While isolating these three categories of job roles represents the ideal model, the small size of some departments inhibits the segregation of duties, especially for low-dollar transactions.

Privilege Management promotes the concept of segregation of duties by showing a warning message on DAs’, Reviewers’, and Approvers’ worklists if a Decentralized Administrator saves the following combinations of privileges for the same person on any resources:

- SigAuth PAF and eDog Transaction Approver
- PA Initiator and PA HD Executor
- eProcurement Creator, SigAuth eProcurement Executor, and eDog Transaction Approver

These combinations of privileges do not have to be entered at the same time to solicit the warning message. However, once all privileges from one of the three combinations are pending or saved and pending for an individual, the worklist warning message will appear.

Decentralized Administrators, Reviewers and Approvers are encouraged to avoid assigning such combinations of privileges when possible.

The warning message on DAs’, Reviewers’, and Approvers’ worklists does not prevent these combinations of privileges from getting saved to a person for the same resource—it only warns the DA, Reviewer or Approver of the risk.
Summary: Entering Privileges into Privilege Management

Flowchart 5-1: Entering Privileges in Privilege Management

Note: The above processes also apply to editing, copying, and moving privileges in a workflow environment.
Unit 6
The Admin Tab

The Admin tab appears for Administrators, Reviewers and Approvers in Privilege Management; however, Decentralized Administrators will use its features more than other administrators. This tab contains the Transfer and Termination reports and a link to the Privilege Management InfoView reports.

Decentralized Administrators should use this tab to generate Transfer and Termination reports weekly to check for transferred and terminated employees in their purview. Using report information, administrators can then determine next steps in managing application access: should an employee’s access be removed entirely, or copied or moved to another employee, etc.?

Section 1: Transfer and Termination Reports

In accordance with the Privilege Management Policies and Procedures, decentralized administrators should review the weekly Transfer and Termination reports to:

- Remove privileges for VUnet IDs who have transferred.
- Remove privileges for VUnet IDs who have terminated but may not have been auto-deleted from Privilege Management.
Transfer Reports

Each Sunday night MIS generates a Transfer Report which captures all persons with a privilege in Privilege Management who underwent a job code and/or home department change during the prior week. This report is not bound by purview; it contains transfer information for all centers and home departments.

The Transfer Report includes the following fields:

- Employee Name
- ID/Record #
- VUnet ID
- Job Code Change (Yes or No)
- Previous Home Department (ID and Name)
- Current Home Department (ID and Name)
- Effective Date- shows when the transfer did or will occur (this can be a past or future date).
- Date of Change- shows when the PAF was processed in the HR system.

To view Transfer Reports:

- Use the drop-down arrow under Report Type to choose Transfer.
- Select the year and month for the report(s). Note that although you’re encouraged to view these reports weekly, you select only the month and year from the drop-down menus. For the month you select, Privilege Management will display all weeks containing reports.
- Click Submit.

When you click Submit, all available reports for the specified time period will appear as links:

To view a report, click its link.
### Vanderbilt University
### Financial Systems
### Employee Transfer Report
10-OCT-2004 thru 16-OCT-2004

<table>
<thead>
<tr>
<th>Employee Name</th>
<th>(ID/Ext #)</th>
<th>VaNet ID</th>
<th>Job Code Change</th>
<th>Previous Dept</th>
<th>Previous Dept Name</th>
<th>Current Dept</th>
<th>Current Dept Name</th>
<th>Effective Date</th>
<th>Date of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Algood, Holly M S</td>
<td>0055866 / 0</td>
<td>ALGOODHM</td>
<td>Yes</td>
<td>104162</td>
<td>Infectious Disease</td>
<td>104162</td>
<td>Vanderbilt School of Medicine</td>
<td>10-01-2004</td>
<td>10-06-2004</td>
</tr>
<tr>
<td>Arndt, Thomas</td>
<td>0011244 / 0</td>
<td>AMINT</td>
<td></td>
<td>104291</td>
<td>Clinical Pharm - Pla</td>
<td>104291</td>
<td>Clinical Pharmacology</td>
<td>10-01-2004</td>
<td>10-12-2004</td>
</tr>
<tr>
<td>Bresen, Jacqueline M</td>
<td>0005863 / 0</td>
<td>BROWNS</td>
<td>Yes</td>
<td>120430</td>
<td>Chemistry</td>
<td>120430</td>
<td>Chemistry</td>
<td>10-08-2004</td>
<td>10-13-2004</td>
</tr>
<tr>
<td>Chappar, Cally R</td>
<td>0004440 / 0</td>
<td>CHAPPCR</td>
<td></td>
<td>119110</td>
<td>Vanderbilt House Care</td>
<td>119110</td>
<td>Vanderbilt House Care</td>
<td>10-01-2004</td>
<td>10-11-2004</td>
</tr>
</tbody>
</table>

**Sample Transfer Report**

To print a report, click **File > Print** from the menu bar.

The privileges of employees who underwent a job code and/or home department change are not automatically deleted from Privilege Management. Instead, this report serves as a notice to identify security access changes that potentially need to be made. Whether follow-up is needed is left up to your discretion as the security administrator.

All job code and /or home department changes will be reported, and changes manually entered by an HR Operator will appear on the report on a timely basis. **There will, however, be a delay in the reporting of automated changes.** This relatively small number of changes is entered through an automated process that will not appear on the report until an HR Operator subsequently performs a manual entry for that individual. Once the manual entry occurs, the report will show the most recent manual entry and the previous automated change for that individual.
Termination Reports

Each Sunday night MIS generates a Termination Report which captures all persons with a privilege in Privilege Management who no longer have any active job code.

The Termination Reports display all of the terminations that occurred within the entire institution for the time period selected. Therefore, you will have to scan the report for terminations that occurred within your area.

The Termination Report includes the following information:

- Employee Name
- Employee ID
- VUnet ID
- Node
- Home Department (ID and Name)
- Auto Deleted (Yes or No)

To view Termination Reports:

- Use the drop-down arrow under Report Type to choose Termination.
- Select the year and month for the report(s). Note that although you’re encouraged to view these reports weekly, you select only the month and year from the drop-down menus. For the month you select, Privilege Management will display all weeks containing reports.
- Click Submit.

When you click Submit, all available reports for the specified time period will appear as links:

Report Type: Termination
Month: October
Year: 2004

October 24, 2004
October 10, 2004
October 17, 2004
October 31, 2004

Termination Reports for October 2004

To view a report, click its link.
Automatic Deletion

The automatic deletion occurs only when the employee’s or student’s status changes from “active” to “inactive” in the Enterprise Person Index (EPI). The EPI is updated with information from the Human Resources System and the Student Records System every 10 minutes. If a user is both an employee and a student, his/her access will not be deleted from the system during the Sunday night process until both the employee and student statuses change from “active” to “inactive.”

If that user becomes an “inactive” employee, but is still an “active” student, none of his/her roles will be deleted, but he/she will be displayed on the report.

If a user has multiple job records, an automatic deletion occurs only if the user has been terminated from all jobs. Users on any kind of leave will not be deleted.

Non-employees (e.g., external auditors, consultants, etc.) are not automatically deleted from Privilege Management when their eDog, eProcurement, Signature Authorization, and/or WALDO security roles are no longer applicable. As a result, departments/divisions are responsible for contacting the appropriate administrator(s) to request the manual removal of non-employee roles.

Section 2: File Upload

A few centralized administrators will also see fields for uploading files into Privilege Management. This feature allows centralized administrators to add numerous privileges for many people in one step. If you have the File Upload Administrator privilege and can therefore see the File Upload fields on the Administrator tab, you can contact Financial Information Systems at fis-applications@vanderbilt.edu for assistance with this process.
Unit 7
Reports Tab

Section 1: Privilege Management Reports in InfoView

From the Reports tab, Privilege Management links to the eBusiness website, where you can log into InfoView XI to generate more Privilege Management reports.

These reports are external to the Privilege Management application because they were created in Business Objects, a reporting application used to create reports for many purposes at Vanderbilt. The Privilege Management reports are published through the InfoView web portal, which allows you to access these reports via the Internet. **You do NOT need to install or learn Business Objects to generate and view the Privilege Management reports**—all work has been done for you in InfoView.

**Accessing the Reports**

If you are not able to log into InfoView, request access to the Business Objects-Privilege Management universe. To do so, complete the Business Objects security request form, posted on the Forms Locator, at [http://www.vanderbilt.edu/stop/forms/uploads/Business_Objects_Security_form.pdf](http://www.vanderbilt.edu/stop/forms/uploads/Business_Objects_Security_form.pdf). Enter *Privilege Management* in the field asking for Universe Requested and submit the completed form to the correct security liaison for your area, listed on page 2 of the form.
Navigating to Privilege Management Reports in InfoView

After clicking the link to Vanderbilt’s eBusiness webpage, click the InfoView XI link on that page.

- Enter your VUnet ID in the user name field and your ePassword in the password field.
- Choose LDAP for Authentication, if it is not already selected.
- Click Log On.
The InfoView home page will appear. (Note that if you’ve previously customized InfoView to change your home page, you will see a different page at this point.)

- Click the plus sign to expand Public Folders. The sub-folders that appear depend on what universes you have access to in Business Objects. Therefore, with the exception of the Privilege Management folder, the folders you see on your screen might differ from the ones pictured in this guide.

- Click the plus sign next to Privilege Management to expand this folder.

- Click the Prod Reports (for Production Reports) folder to see all the Privilege Management reports available.

**Navigating to the Privilege Management Reports in InfoView**
If you do not see a folder for Privilege Management reports under Public Folders, request access to the Business Objects-Privilege Management universe. See page 75 for more information on requesting access to the Privilege Management universe for Business Objects.

When you click the Prod Reports folder, the available Privilege Management reports will appear in a window on the right side of the screen.

*Privilege Management Reports in InfoView*
Reports

The following reports are available in InfoView to help you manage privileges for your area:

- **Audit Trail by Administrator** - shows you all activity in Privilege Management by the PM administrator that you specify. It includes, by employee, all privilege assignments and deletions on all resources.
  - To generate this report, click its title.
  - In the light blue prompts pane that appears, enter the following information:
    - Enter the Privilege Management administrator's VUnet ID in ALL CAPS.
    - Enter a start and end date in the corresponding fields.
    - Click the Run button.

---

**Sample Audit Trail by Admin Report**

### Roles Administered By: WILLIAJC  Williams, Jeremy C

<table>
<thead>
<tr>
<th>Employee Name: last, first</th>
<th>VUnet ID</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Action</th>
<th>Node</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/21/08 02:16:44 PM</td>
<td>ADD</td>
<td>1551200000</td>
<td>BO Corp Viewer - APPO</td>
</tr>
<tr>
<td>05/21/08 02:25:32 PM</td>
<td>ADD</td>
<td>1551200000</td>
<td>BO Corp Viewer - General Ledger</td>
</tr>
<tr>
<td>05/21/08 02:25:36 PM</td>
<td>DEL</td>
<td>1551200000</td>
<td>BO Corp Viewer - APPO</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Employee Name: last, first</th>
<th>VUnet ID</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Action</th>
<th>Node</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>04/11/08 01:30:12 PM</td>
<td>ADD</td>
<td>1553100000</td>
<td>BO Corp Viewer - APPO</td>
</tr>
</tbody>
</table>

Names and VUnet IDs omitted from sample reports.

Sample Audit Trail by Admin Report
• **Audit Trail by User** - allows you to specify a Privilege Management user, and shows all privilege assignments and changes that any administrators have made for him/her.
  - To generate this report, click its title.
  - In the light blue prompts pane that appears, enter the VUnet ID of the person for whom to view privileges and click Run.

![User Prompt Input]

Enter the Privilege Management user's VUnet ID in **ALL CAPS**.
Click the Run button.

---

**Audit Trail by User**

**Privileges Held By:** VUnet ID  Employee Name: last, first m

**BO Corp Viewer - General L**

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Node</th>
<th>Action</th>
<th>Admin Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/12/08, 05:16:37 PM</td>
<td>1551100000</td>
<td>DEL</td>
<td>McGlasson, Matthew R</td>
</tr>
<tr>
<td>05/12/08, 06:29:07 PM</td>
<td>1551100000</td>
<td>ADD</td>
<td>McGlasson, Matthew R</td>
</tr>
<tr>
<td>05/12/08, 06:29:08 PM</td>
<td>1551100000</td>
<td>ADD</td>
<td>McGlasson, Matthew R</td>
</tr>
<tr>
<td>05/12/08, 06:29:14 PM</td>
<td>1551100000</td>
<td>DEL</td>
<td>McGlasson, Matthew R</td>
</tr>
<tr>
<td>05/12/08, 06:39:20 PM</td>
<td>1551100000</td>
<td>DEL</td>
<td>McGlasson, Matthew R</td>
</tr>
<tr>
<td>05/12/08, 06:49:23 PM</td>
<td>1551100000</td>
<td>ADD</td>
<td>McGlasson, Matthew R</td>
</tr>
</tbody>
</table>

**eDog Administrator**

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Node</th>
<th>Action</th>
<th>Admin Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/12/08, 05:18:03 PM</td>
<td>W22810</td>
<td>ADD</td>
<td>McGlasson, Matthew R</td>
</tr>
<tr>
<td>05/12/08, 06:39:36 PM</td>
<td>W22810</td>
<td>DEL</td>
<td>McGlasson, Matthew R</td>
</tr>
</tbody>
</table>

*Names and VUnet IDs omitted from sample reports.*

*Sample Audit Trail by User Report*
• **Audit Trail by User with Attributes**- allows you to specify a Privilege Management user, and shows all privilege assignments—including attributes—and changes that any administrators have made for him/her.
  - To generate this report, click its title.
  - In the light blue prompts pane that appears, enter the VUnet ID of the person for whom to view privileges (as illustrated above) and click run.

![Audit Trail by User with Attributes](image)

**Employee Name: last, first m**

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Action</th>
<th>Role</th>
<th>Node</th>
<th>Attribute Name</th>
<th>New Attr Value</th>
<th>Old Attr Value</th>
<th>Admin Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/23/05, 02:27:47 PM</td>
<td>DEL</td>
<td>eProcurement Reviewer</td>
<td>1051100000</td>
<td>Dollar Limit</td>
<td>All</td>
<td></td>
<td>Smith, Kimberly K</td>
</tr>
<tr>
<td>06/23/05, 02:27:47 PM</td>
<td>DEL</td>
<td>eProcurement Reviewer</td>
<td>1051100000</td>
<td>Federal Indicator</td>
<td>All</td>
<td></td>
<td>Smith, Kimberly K</td>
</tr>
<tr>
<td>06/23/05, 04:53:41 PM</td>
<td>ADD</td>
<td>eProcurement Reviewer</td>
<td>1051100000</td>
<td>Fund Type</td>
<td>All</td>
<td></td>
<td>Smith, Kimberly K</td>
</tr>
<tr>
<td>06/23/05, 04:53:41 PM</td>
<td>ADD</td>
<td>eProcurement Reviewer</td>
<td>1051100000</td>
<td>Dollar Limit</td>
<td>All</td>
<td></td>
<td>Smith, Kimberly K</td>
</tr>
<tr>
<td>06/23/05, 04:53:41 PM</td>
<td>ADD</td>
<td>eProcurement Reviewer</td>
<td>1051100000</td>
<td>Federal Indicator</td>
<td>All</td>
<td></td>
<td>Smith, Kimberly K</td>
</tr>
<tr>
<td>06/23/05, 04:53:41 PM</td>
<td>ADD</td>
<td>eProcurement Reviewer</td>
<td>1051100000</td>
<td>Fund Type</td>
<td>All</td>
<td></td>
<td>Smith, Kimberly K</td>
</tr>
<tr>
<td>06/23/05, 04:53:41 PM</td>
<td>ADD</td>
<td>eProcurement Reviewer</td>
<td>1051100000</td>
<td>Dollar Limit</td>
<td>All</td>
<td></td>
<td>Smith, Kimberly K</td>
</tr>
<tr>
<td>06/23/05, 04:53:41 PM</td>
<td>ADD</td>
<td>eProcurement Reviewer</td>
<td>1051100000</td>
<td>Federal Indicator</td>
<td>All</td>
<td></td>
<td>Smith, Kimberly K</td>
</tr>
<tr>
<td>06/23/05, 04:53:41 PM</td>
<td>ADD</td>
<td>eProcurement Reviewer</td>
<td>1051100000</td>
<td>Fund Type</td>
<td>All</td>
<td></td>
<td>Smith, Kimberly K</td>
</tr>
<tr>
<td>06/04/05, 09:01:41 AM</td>
<td>ADD</td>
<td>eProcurement Reviewer</td>
<td>1051100000</td>
<td>Dollar Limit</td>
<td>All</td>
<td></td>
<td>Smith, Kimberly K</td>
</tr>
<tr>
<td>06/04/05, 09:01:41 AM</td>
<td>ADD</td>
<td>eProcurement Reviewer</td>
<td>1051100000</td>
<td>Federal Indicator</td>
<td>All</td>
<td></td>
<td>Smith, Kimberly K</td>
</tr>
<tr>
<td>06/04/05, 09:01:41 AM</td>
<td>ADD</td>
<td>eProcurement Reviewer</td>
<td>1051100000</td>
<td>Fund Type</td>
<td>All</td>
<td></td>
<td>Smith, Kimberly K</td>
</tr>
<tr>
<td>04/02/07, 12:52:22 PM</td>
<td>ADD</td>
<td>egl Viewer</td>
<td>1401600000</td>
<td></td>
<td></td>
<td></td>
<td>McCluskey, Matthew H</td>
</tr>
</tbody>
</table>

Names omitted from sample reports.

**Sample Audit Trail by User with Attributes Report**

• **Privileges by Resource**- shows the people and privileges assigned to the resources you specify.
  - To generate this report, click its title.
  - In the open field on the left side of the prompts window, type in the name or number of the resource for which to view privilege assignments, or select the resource from the pick-list. Resources are NOT limited by purview.
  - You can use the binoculars to search for a resource.
  - To select a resource for use, click the double arrows pointing to the right. This action will move the resource to the window on the right. (You do not have to remove the XXXXXXXXXXX prompt from this window before generating a report.)
  - To select multiple resources in consecutive order, click the first resource, hold the shift key and click the last resource. To select multiple resources that are not in consecutive order, hold the Ctrl key while clicking the desired resources.
  - Click **Run Query** to generate the report.
Prompts for Privileges by Resource Report

Sample Privileges by Resource Report

Names and VUnet IDs omitted from sample reports

Privileges for the selected resource are organized by tab on this report.
• **Privileges by Person** - for the people you specify, this report shows all resources and privileges to which the people are assigned.
  - To generate this report, click its title.
  - In the open field on the left side of the prompts window, type in the name of the person in ALL CAPS for whom to view privilege assignments, or select the person from the pick-list.
  - You can use the binoculars to search for a person.
  - To select a person, click the double arrows pointing to the right. This action will move the VUnet ID to the window on the right.
  - To select multiple people in consecutive order, click the first person, hold the shift key and click the last person. To select multiple people that are not in consecutive order, hold the Ctrl key while clicking the desired names/VUnet IDs.
  - Click Run Query to generate the report.

![Prompts for Privileges by Person Report](image)
Sample Privileges by Person Report- Privileges Tab

The above example shows the Privileges tab of the report.

The next tab, eProcurement Creator List, shows a list of anyone you included in your report who is also an eProcurement Creator.

The All Direct Assignments tab shows the report information in a single table to facilitate data export.

- **Waldo Viewer Additions** - shows everyone assigned the Waldo viewer privilege.
  - To generate this report, click its title.
  - In the open field on the left side of the prompts window, type in the name of the person in ALL CAPS for whom to view privilege assignments, or select the person from the pick-list.
  - You can use the binoculars to search for a person.

To select a person, click the double arrows pointing to the right. This action will move the VUnet ID to the window.

**Reports Under Development**

The following reports are under development and will be published in the near future:

- **Assignments with Target End Dates** - report shows all privileges with a Target End Date within the date range specified upon generating the report. Administrators can use this report as a list of privileges to suspend, reinstate, delete or edit.

- **Export of Resources and Privileges** - includes a hierarchical listing of each resource, resource type (center, sumto center, home department, etc.), resource name and all VUnet IDs, assignee names, privileges, and attributes assigned to the resource you specify.
• Assignments with Segregation of Duties Warning- shows all privilege assignments that contain any one of the three combinations of privileges that yield the Segregation of Duties warning message on a worklist in Privilege Management (see page 68 for more information). This report includes anyone with these assignments—not just those currently on a worklist.
Unit 6
Help and Logout

All users can access the Help and Logout tabs at the top of the screen.

Help
Click the Help tab to access the Privilege Management User Guide. You can use the guide as an online resource or save it to your computer as a PDF file.

Logout
Click the Logout tab to end your session in Privilege Management. To prevent possible connection errors with the database if you reenter Privilege Management, it is recommended that you click Logout before exiting as opposed to closing your browser.
APPENDICES

Updates to Privilege Management

Updates to Resources
Privilege Management receives low-level center and home department information from the General Ledger and PeopleSoft applications, respectively. If updates occur to these systems, Privilege Management will also be affected. If the roll-ups of resources change in the General Ledger or PeopleSoft, changes can take one day or one week to be reflected within Privilege Management.

Daily Updates
Once a cost center is added in the General Ledger system, it will be available the next day in Privilege Management for viewing and making privilege assignments.

For eProcurement and Signature Authorization: note that once the new centers are added to the General Ledger, there will be at least a one-day delay before an administrator can add privileges to these new centers in Privilege Management to allow purchasing.

Weekly Updates
The following data come from various systems that update Privilege Management weekly. Therefore, these resources’ changes will appear in Privilege Management the subsequent Monday:

- Home Department
- Major Operating Division
- PCC Sum
- Function

Changes to Resource Groups
Changes to high-level resource groupings require manual updates by the application managers of the contributors to Privilege Management (i.e., the General Ledger and PeopleSoft). To change roll-ups in Privilege Management, contact the appropriate central office.

Updates to Privilege Assignments
Any privilege assignments you administer are immediately reflected in Privilege Management and in the application(s) to which the privileges apply. For example, if you give someone the eDog Viewer privilege on a particular center, he/she will be able to log into eDog immediately to view eDog reports for that center.
Decentralized Administrator Tasks in Privilege Management

As a Privilege Management Decentralized Administrator, your actions are governed by the Policies and Procedures posted at [http://www.vanderbilt.edu/fis/Apps/pm.htm](http://www.vanderbilt.edu/fis/Apps/pm.htm). This document contains detailed instructions the following critical tasks:

- Processing security requests.
- Addressing transferred, terminated and medical LOA employees.
- Performing annual privileges review.

**Monthly Tasks**
- Generate Transfer and Termination reports.
  - Remove privileges for any terminated employees, transferred, and medical LOA employees who no longer need their current roles.
- Generate Target End Date reports (if your department uses this feature) for the upcoming month.
  - For any privileges that have a Target End Date set to the next month, follow up with others in your department to determine if any actions should be taken on the privileges in Privilege Management.

**Annual Task**
- Export data for your purview and review all assignments to resources within your purview.

**Tasks to Perform on an As-Needed Basis**
- Process security requests for employees adding or deleting role privileges.
- Use Business Objects to generate reports from the PM universe to monitor the following information:
  - All privileges on a resource.
  - All privileges assigned to each person.
  - All actions performed by a particular PM administrator.
  - The privilege assignment history for a designated person.
How Copying or Moving Privileges Affects a Privilege Status

Privileges do not have to be active to be selected for copying or moving. The table below shows what happens to a privilege’s status when it is copied or moved to another person in both workflow and non-workflow situations.

The source person refers to the person already possessing the privilege(s) that will be copied or moved; the target person refers to the person who will receive one or more new privileges as a result of the copy or move.

<table>
<thead>
<tr>
<th>Status of Privilege for Source Person</th>
<th>Status of Privilege for Target Person</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Pending</td>
</tr>
<tr>
<td></td>
<td>Active</td>
</tr>
<tr>
<td>Suspended</td>
<td>Suspended; privilege will change to pending once it’s reinstated.</td>
</tr>
<tr>
<td></td>
<td>Suspended; privilege will change to active once it’s reinstated.</td>
</tr>
<tr>
<td>Pending</td>
<td>Pending</td>
</tr>
<tr>
<td></td>
<td>Active</td>
</tr>
<tr>
<td>*Only an Application Admin—not Decentralized Admin—could perform a copy/move on a pending privilege outside of workflow.</td>
<td></td>
</tr>
<tr>
<td>Rejected</td>
<td>Pending</td>
</tr>
<tr>
<td></td>
<td>Active</td>
</tr>
<tr>
<td>*Only an Application Admin—not Decentralized Admin—could perform a copy/move on a rejected privilege outside of workflow.</td>
<td></td>
</tr>
</tbody>
</table>

Refer to page 45 for information on suspending and reinstating privileges.
Refer to page 60 for information on workflow and pending and rejected privileges.
Roles and Access in Privilege Management

The tabs and buttons you see in Privilege Management vary depending on your roles in the application. The table below provides a summary of what tabs different types of roles can access in Privilege Management.

<table>
<thead>
<tr>
<th>Role</th>
<th>Admin &amp; Reports</th>
<th>My Purview</th>
<th>My Worklist</th>
<th>My Privileges</th>
<th>Resource</th>
<th>Person</th>
<th>Help/Logout</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Reviewer/Approver</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>End user with at least one active privilege in Privilege Management</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Privileges, Definitions, and Categories

A current and complete list of all privileges and their definitions and categories is posted online at http://www.vanderbilt.edu/fis/Apps/pm.htm.
ePAC Privileges in Privilege Management

Administrators who can add or change ePAC privileges should be aware that changes to the following privileges in Privilege Management can freeze PACs that are in progress in ePAC:

<table>
<thead>
<tr>
<th>ePAC Privilege</th>
<th>Privilege Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>PA Initiator</td>
<td>Enables holder to create, save, edit and submit all Personnel Action Changes, which starts the approval process in the ePAC web application.</td>
</tr>
<tr>
<td>PA Reviewer</td>
<td>Enables holder to view and make comments on Personnel Action Changes in ePAC web application. This includes two roles: Required and Optional. Required Reviewer provides a level of approval for a PAC to continue in workflow.</td>
</tr>
<tr>
<td>PA HD Executor</td>
<td>Enables holder to update, approve or reject Personnel Action Changes in ePAC web application. Review serves as the final level of departmental approval.</td>
</tr>
<tr>
<td>SigAuth PAF</td>
<td>Enables holder to approve financial transactions processed through Personnel Action Changes (paper form or ePAC), Payroll Check Distribution Authorization Forms (paper form), and Home Department Change Forms (paper form), which establish pay rate and job.</td>
</tr>
<tr>
<td>Cost Transfer Approver</td>
<td>Enables holder to review, approve or reject retroactive earnings distribution changes only. This is the approval that completes the cost transfer in the ePAC web application.</td>
</tr>
<tr>
<td>PA Accountant</td>
<td>Enables holder to perform staff accounting review for Retroactive Distribution changes in ePAC web application. Able to review, approve or reject retroactive earnings distribution changes only.</td>
</tr>
<tr>
<td>PA BRET Executor</td>
<td>Enables holder to approve Terminations, Job Code, Pay Rate and Standard Hours changes for Post-Doc, Visiting Research, Research Intern Undergrad, and Research Intern Graduates in the ePAC web application.</td>
</tr>
<tr>
<td>PA Comp Executor</td>
<td>Enables holder to approve or reject PACs that have job codes that were selected by Compensation as needing final Compensation approval in the ePAC web application.</td>
</tr>
<tr>
<td>PA GME Executor</td>
<td>Enables holder to approve Terminations, Job Code, Pay Rate and Standard Hours changes for Residents and Clinical Fellows in ePAC web application.</td>
</tr>
<tr>
<td>PA Initiator Central</td>
<td>Enables holder to create, save, edit and submit retro distribution changes that will bypass departmental workflow and advance directly to the PAC Accountant in the ePAC web application.</td>
</tr>
<tr>
<td>PA JPP Executor</td>
<td>Enables holder to provide final approval for an entity that is neither the Home Department, nor an affected Cost Center. The role is invoked on; Job Code, Position, Pay Rate and Standard Hours changes on both Filled and Vacant PACs in the ePAC web application.</td>
</tr>
<tr>
<td>PA Workflow Admin</td>
<td>Enables holder to set the Processing Deadline Date for the ePAC web application, or reassign effort certification, or complete workflow for a distribution change where effort has not been certified. Actions are based on which role attribute is assigned.</td>
</tr>
</tbody>
</table>

If the person who possesses one of the above privileges is attached to a PAF that’s in progress in ePAC, and that person’s related ePAC privilege is changed or deleted in Privilege Management, the PAC will “freeze” in ePAC. To avoid this situation, wait until after a payroll deadline to change the ePAC privilege.
Glossary of Terms

The below terms relate to the Privilege Management application and its use:

- **Center**- a 10-digit cost center used in the General Ledger. Privilege Management uses centers and higher-level groupings of centers for many privilege assignments.

- **Home Department**- derives from HR’s PeopleSoft application, which is Vanderbilt’s personnel management system. Privilege Management uses home departments and higher-level groupings of home departments for assigning many HR-related privileges (e.g., ePAC privileges).

- **Inheritance**- access to a resource by virtue of access to another resource that is higher in the financial or organizational structure.
  - Example: If you have an assigned privilege at a sumto center, you automatically have the same assigned privilege on all centers that roll-up to that sumto center, even though your VUnet ID is not explicitly assigned to each center.

- **Privilege**- describes any viewing, transactional, or administration role that can be assigned to an individual on a resource. For a comprehensive listing of Privileges available in Privilege Management and detailed explanations of each, go to the following webpage: [http://www.vanderbilt.edu/fis/Documents/PM/All%20Privileges.xls](http://www.vanderbilt.edu/fis/Documents/PM/All%20Privileges.xls).

- **Purview**- the resources for which an administrator can grant privileges or for which a Privilege Reviewer or Privilege Approver can approve privileges.

- **Resource**- an entity in Privilege Management where a privilege can be assigned. Common examples include centers, home departments and sumtos.

- **Sumto Center**- alphanumeric field with six or fewer characters that represents the summary of a group of cost centers.

- **Sumto Home Department**- alpha field with six characters that represents the summary of a group of home departments.

- **Workflow**- process in Privilege Management where an assigned privilege must first be approved or rejected by a Decentralized Administrator Executor before becoming active.