Bravura Privilege:

Requesting Privileged Account Access

This document demonstrates how regular users use the *Privileged access* app and authorization workflow to request privileged account access.

This document contains:

- Requirement
- Solution
- Use case: Requesting Windows account access
- Use case: Requesting Unix account access

1 Requirement

Staff often require temporary access to privileged accounts or elevated privileges to complete tasks. Sharing passwords that rarely change poses a security risk. Staff access should be authorized, auditable, and passwords should be randomized often.

2 Solution

The *Privileged access* app allows regular users to request temporary access to privileges. Authorizers are notified, and if they approve the request, the user can *check out* the access privilege, then *check in* when the access is no longer needed, or after a set time. Upon check-in, passwords are randomized.

3   Use case: Requesting Windows account access

This use case demonstrates how:

1. End users request to check out the Windows administrator account.

2. Authorizers approve the request.

3. End users check the account back in.

Requirements

This use case requires:

- *Hitachi ID Bravura Privilege* and *Hitachi ID Connector Pack* installed

- *Hitachi ID Bravura Pattern: Privileged Access Edition* installed

- Active Directory source of profiles

- Teams set up

- Managed Systems onboarded

- Managed accounts onboarded

In this case, teams are set up to allow the user to request to check out Windows or Linux administrator managed accounts.
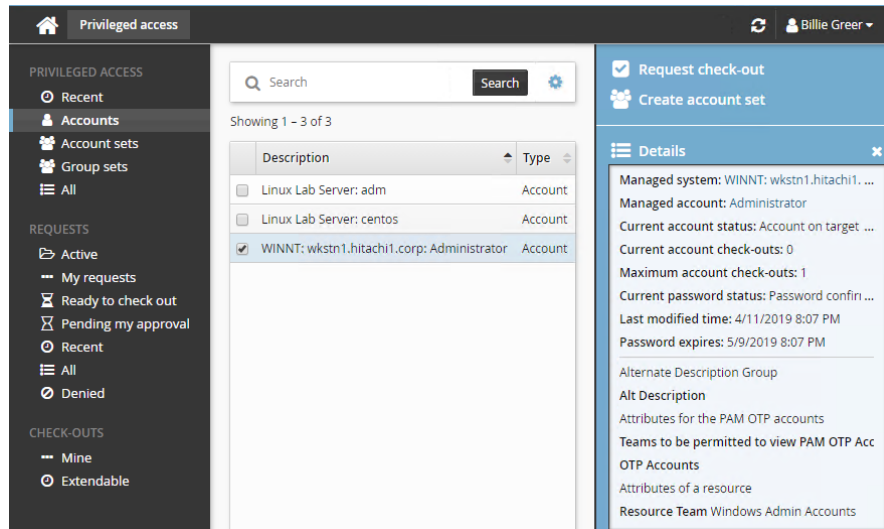
The approver group for "Windows Admin Accounts" is set up so that a request to check out a Windows administrator account needs approval from a member of the IT-WINDOWS-MANAGERS group. Requests to check Linux managed accounts need to be approved from a member of the IT-UNIX-MANAGERS group, as configured for the "Unix Admin Accounts" team.

Request to check out the Windows admin account

1. Log in to *Bravura Privilege* as the requester.

2. Click **Privileged access**.

   The *Privileged access* app opens.

3. Click **Accounts** under the PRIVILEGED ACCESS heading from the Filter panel to see available accounts.
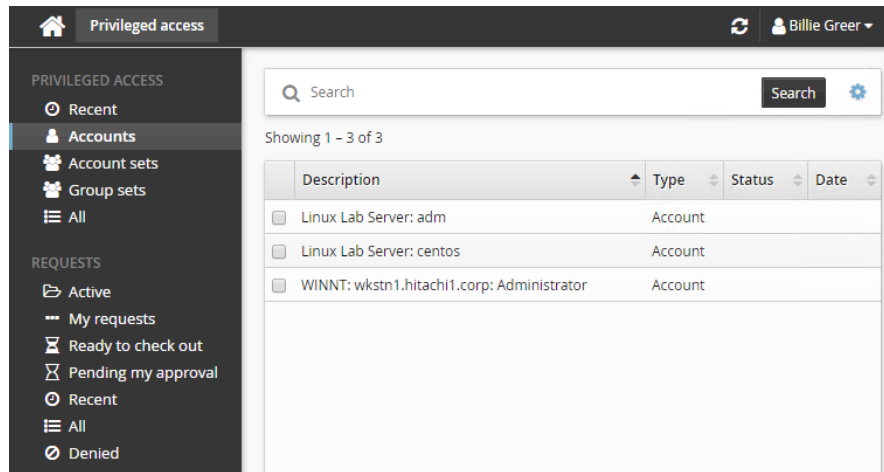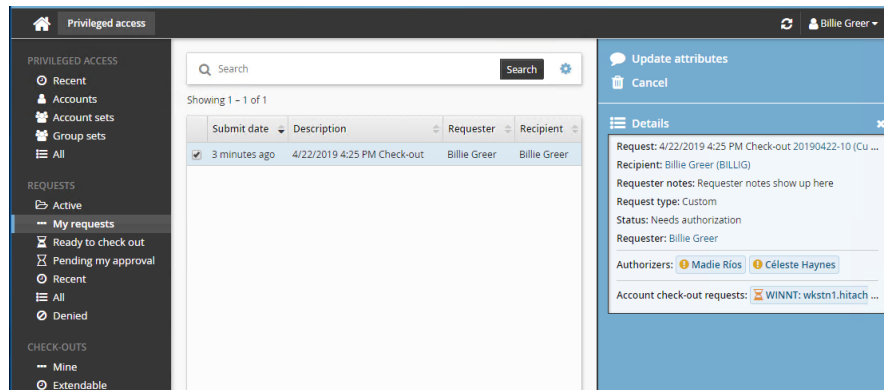
4. Select the account to request access.

5. Click **Request check-out** from the Actions panel to open the request details form.

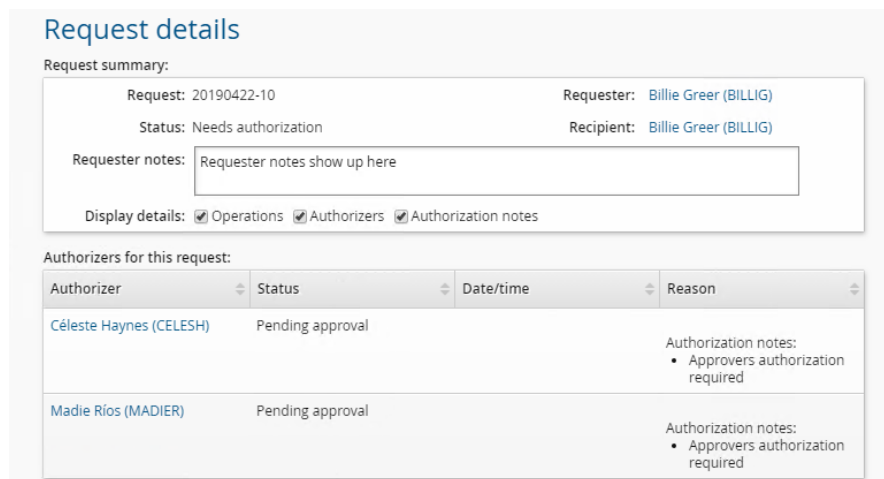6. Review the required information for the request.

7. Enter any **Requester notes** that you would like displayed to the authorizers.

8. Click the **Submit** button at the bottom of the request details form.

   Bravura Privilege issues the request, notifies appropriate authorizers, and displays a summary of the request.
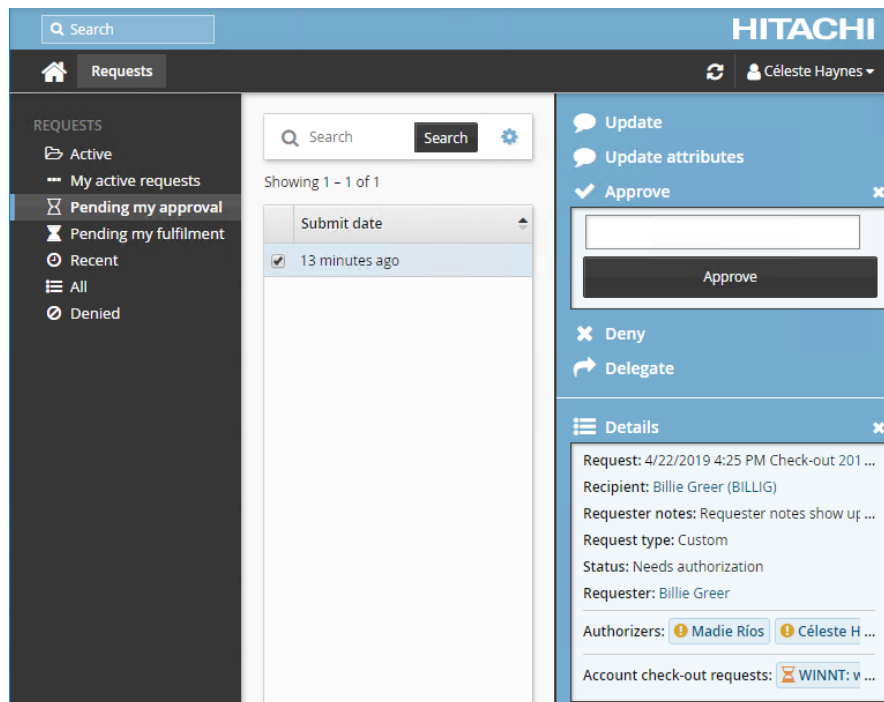
3

9. Open the request details and check the boxes at the top of the request for **Operations**, **Authorizers** and **Authorization notes** to review the available authorizers.

Authorize the request

To authorize the request:

1. Log in to *Bravura Privilege* as the authorizer.

2. Click the link: **There are 1 request(s) awaiting your approval**.
   The *Requests* app opens.

3. From the Results panel, select the request you want to review.
   Hitachi ID Bravura Privilege displays the details in the Actions panel panel on the right.

4. Review the request.
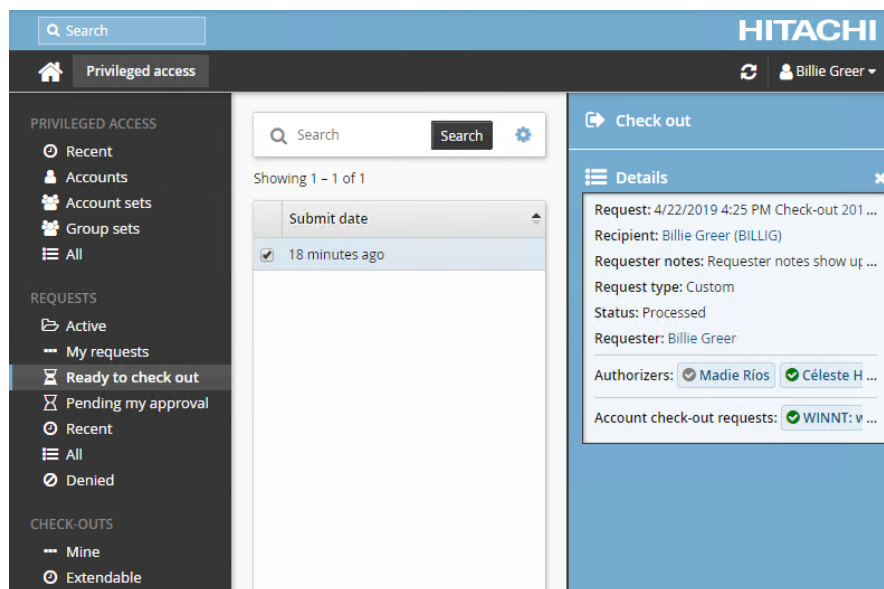
5. Click **Approve**.

6. Click the **Approve** button below the notes field.

Check out the managed account

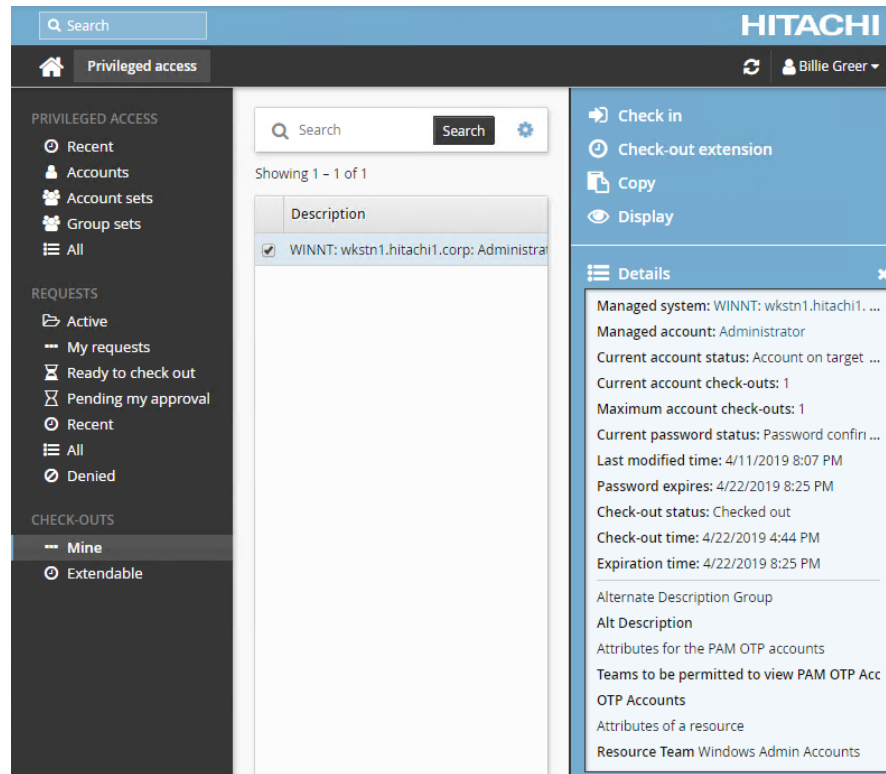Once the request has been approved, you can check out the account:

1. Log in to *Bravura Privilege* as the requester.
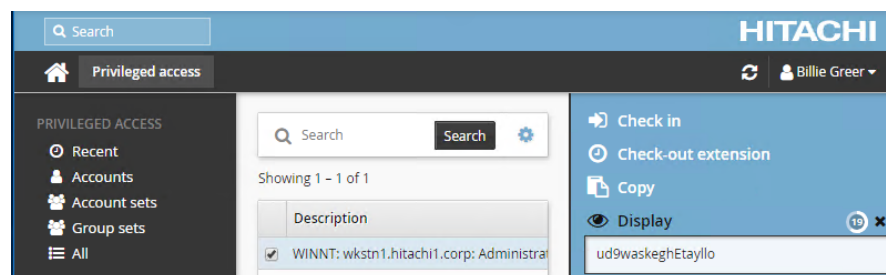2. Click the link **Your privileged access requests have been approved**.

3. Select the account from the Results panel.

4. Click **Check out** from Actions panel.

   The *Privileged access* app displays available actions in the Actions panel to the right.

5. To view the password, click **Display**.

Check in

Once you have finished using the account, you can check it in again.

1. As the requester, navigate to the *Privileged access* app.

2. Click **Mine** under the CHECK-OUTS heading.
   Select the account from the Results panel to display the check-out details in the Actions panel.

6

3. Click **Check in** from the Actions panel.

   The password is randomized and the account checked back in.

4   Use case: Requesting Unix account access

In this use case you will request to check out the Linux administrator account, authorize the request, check out the account and use it in PuTTy, and then check the account back in.

Requirements

This use case requires:

- *Hitachi ID Bravura Privilege* and *Hitachi ID Connector Pack* installed

- *Hitachi ID Bravura Pattern: Privileged Access Edition* installed

- Active Directory source of profiles

- Global teams set up

- Windows and Linux managed systems onboarded

- Managed accounts onboarded

Request to check out a Unix admin account

1. Log in to *Bravura Privilege* as the requester.

2. Click **Privileged access**.

   The *Privileged access* app opens.

3. Click **Accounts** under the PRIVILEGED ACCESS heading from the Filter panel to see available accounts.
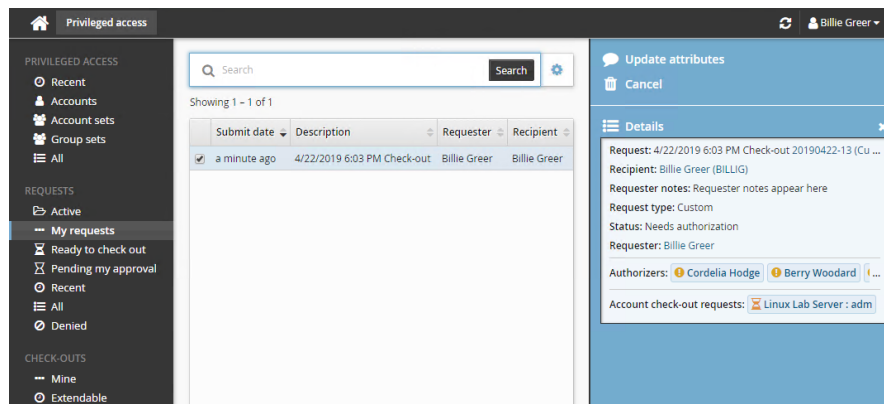

---
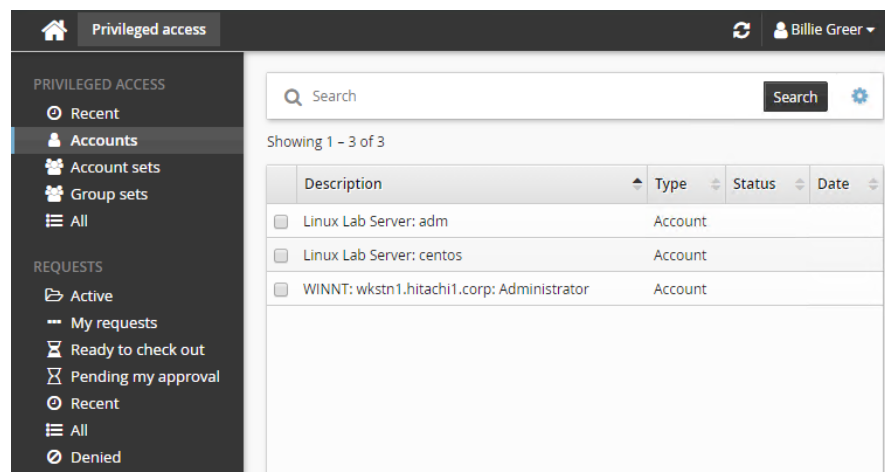
4. Select the user to request access.
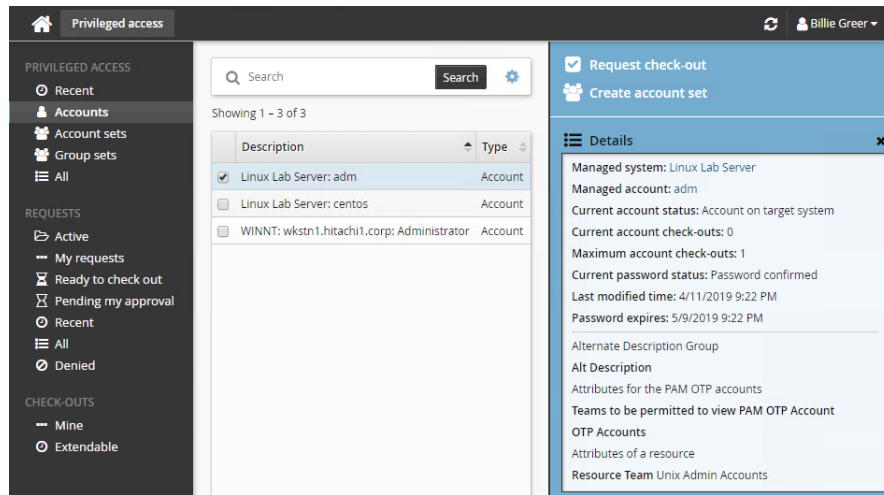
5. Click **Request check-out** from the Actions panel to open the request details form.

6. Review the required information for the request.

7. Enter any **Requester notes** that you would like displayed to the authorizers.

8. Click the **Submit** button at the bottom of the request details form.

   Bravura Privilege issues the request, notifies appropriate authorizers, and displays a summary of the request.

9. Open the request details and check the boxes at the top of the request for **Operations**, **Authorizers** and **Authorization notes** to review the available authorizers.

Authorize the request

To authorize the request:

1. Log in to *Bravura Privilege* as the authorizer.

2. Click the link: **There are 1 request(s) awaiting your approval**.
   The *Requests* app opens.

3. From the Results panel, select the request you want to review.
   Hitachi ID Bravura Privilege displays the details in the Actions panel panel on the right.

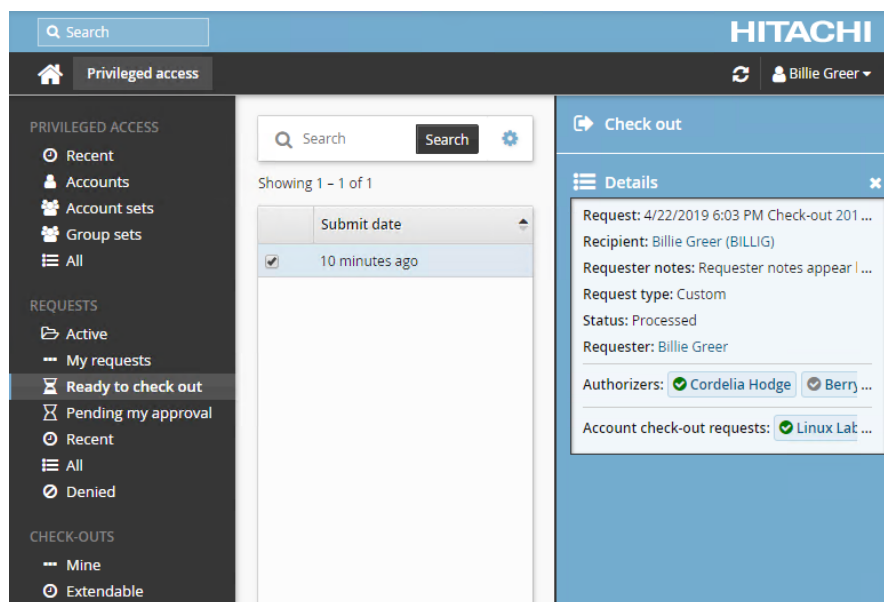4. Review the request.

5. Click **Approve**.

6. Click the **Approve** button below the notes field.

Check out the managed account

Once the request has been approved, you can check out the account:
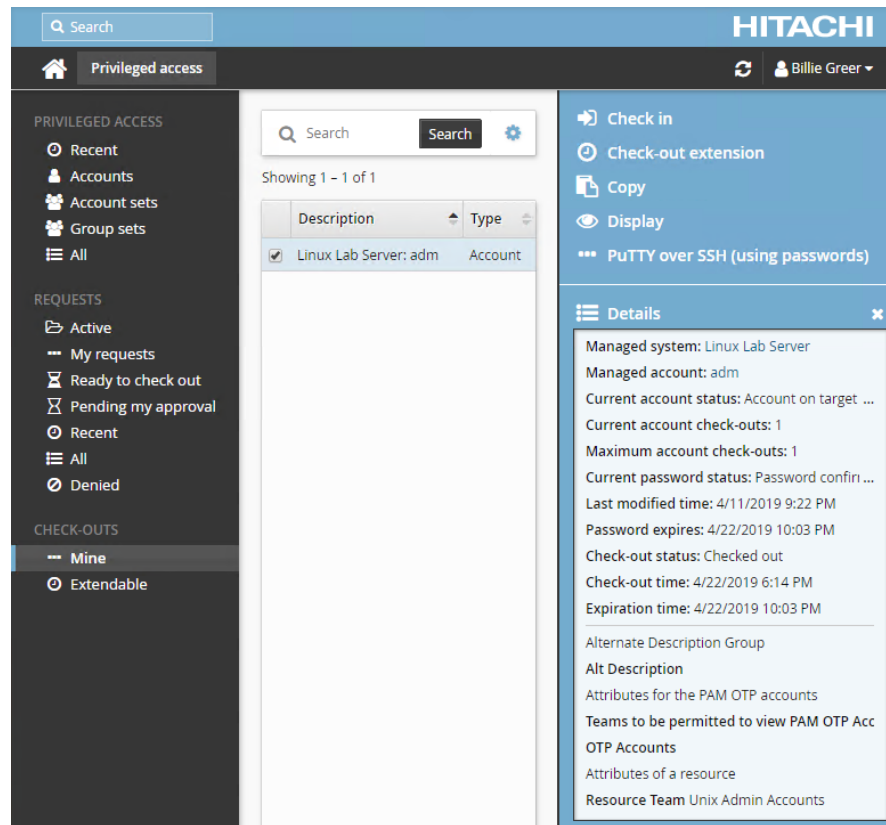
1. Log in to *Bravura Privilege* as the requester.

2. Click the link **Your privileged access requests have been approved**.

3. Select the account from the Results panel.

4. Click **Check out** from Actions panel.

   The *Privileged access* app displays available actions in the Actions panel to the right.


5. To sign on with the account without needing to view the password and log in manually, click **PuTTY over SSH (using passwords)**.

6. You will be prompted to install the extension.

7. Close the extension browser tab once you have the extension installed.

8. When you return to the account checkout, you will see the wording for the extension option has changed to **Install native extension**.
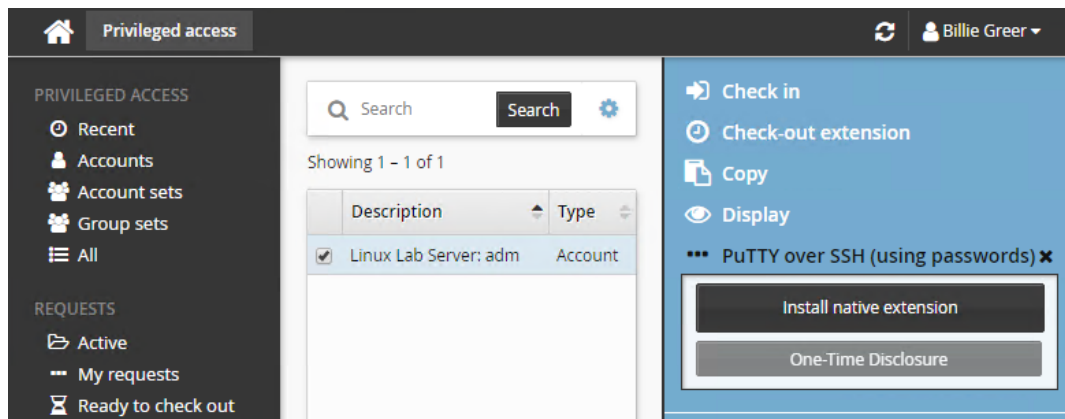
9. Click **Install native extension** and run the `browser-extension-win-x86.msi` after it has been downloaded.

10. Click **Next** on the browser extension setup.

11. Check the box for `I accept the terms in the License Agreement` and click **Next**.

12. Select the option for **Install for all users of the machine** and click **Next**.

13. Click **Typical** as the setup type.

14. Click **Install** and then click **Next**.

15. Complete the installation by clicking **Finish**.

16. Close all of your internet browsers and reopen them again.

17. Log in to *Bravura Privilege* as the requester.

18. Click **Privileged access**.

    The *Privileged access* app opens.

19. Click **Mine** under the CHECK-OUTS heading.

    Select the account from the Results panel to display the check-out details in the Actions panel.

20. Click **PuTTY over SSH (using passwords)**.

    An SSH terminal will open with a PuTTY Security Alert

21. Click **Yes** for the request to cache the server's host key.
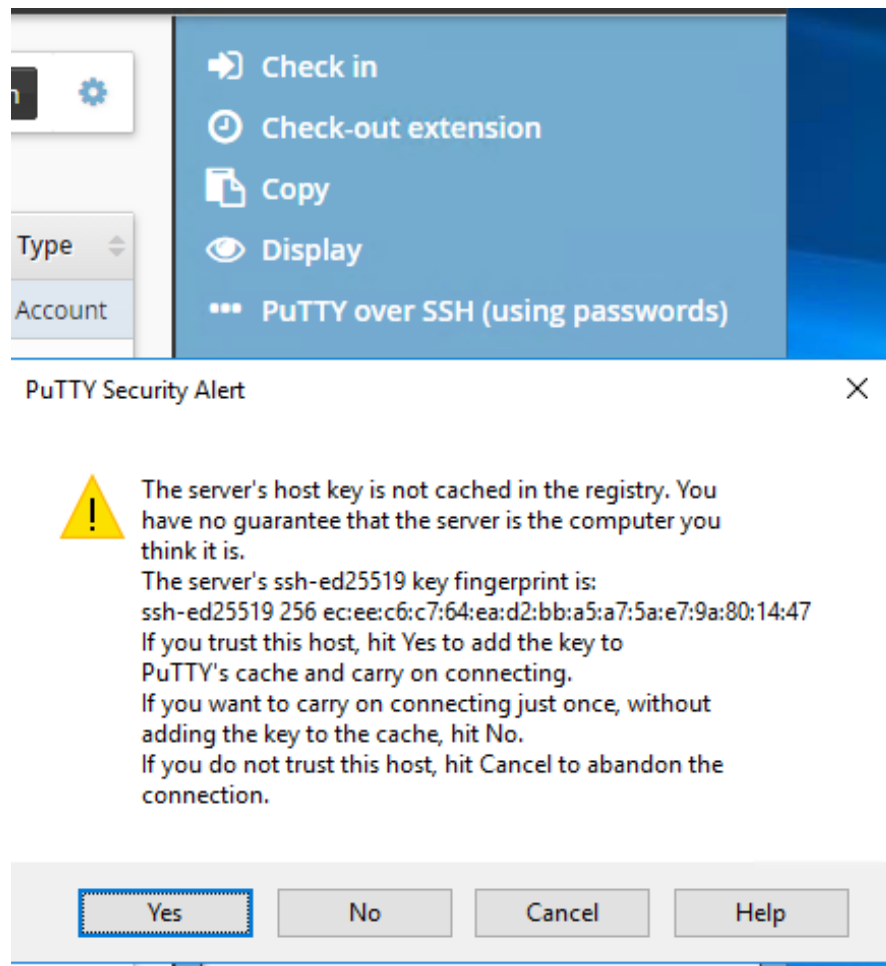
Check in

Once you have finished using the account, you can check it in again.

1. As the requester, navigate to the *Privileged access* app if you are not there already.

2. Click **Mine** under the CHECK-OUTS heading.

   Select the account from the Results panel to display the check-out details in the Actions panel.

3. Click **Check in** from the Actions panel.

   The password is randomized and the account checked back in.