Authorization Checks

Many methods and operations offered by udisks requires the calling user to be sufficiently authorized. Whether the user is authorized is checked using polkit allowing the administrator to configure fine-grained permissions via polkit authorization rules.

There is not necessarily a one-to-one relationship between D-Bus methods and polkit actions - typically the relationship is more complicated and depends on both the context of the process invoking the method, the object the method is acting on and possibly more factors. For example, the Filesystem.Mount() method call may check that the caller is authorized for one of the four actions *org.freedesktop.UDisks2.filesystem-mount*, *org.freedesktop.UDisks2.filesystem-mount-system*, *org.freedesktop.UDisks2.filesystem-mount-other-seat* or *org.freedesktop.UDisks2.filesystem-mount-fstab* depending on circumstances.

Often there will be two polkit actions for one operation - one for so-called “system devices” and one for non-system devices. In this context “system device” refers to the value of the Block:HintSystem D-Bus property and is normally only `TRUE` for devices not considered “removable” (devices considered removable include USB attached storage, Flash media and optical drives). See udisks(8) for how to control if a device is considered a system device.

The polkit actions are not considered stable and may change from release to release so administrators should take notice when upgrading from one version of udisks to another. For example, polkit authorization rules may need to be updated to match an updated policy.

See Table 1, “Known polkit variables” for the variables that can be used to assist in determining if the caller is authorized (note that each variable may not be set for request). For example, a polkit authorization rule for any of the *org.freedesktop.UDisks2.filesystem-mount** actions can use the `device` variable to determine if the caller is authorized to mount a specific block device.

Table 1. Known polkit variables

key	value
`device`	If the object is a block device, this property is set to the value of the Block:PreferredDevice property. If set, this is guaranteed to be a device file, for example “/dev/vg_lucifer/lv_root” or “/dev/sda1”. If the object is not a block device, this is not set.

key	value
`drive`	Like the `device` variable, but if the object is also a drive, this variable includes Vital Product Data about the drive such as the vendor and model identifiers (if available), for example “INTEL SSDSA2MH080G1GC (/dev/sda1)”. Otherwise is just set to the same value as `device`. If the object is not a block device, this is not set (it is however set if the object is a block device but not a drive).
`drive.wwn`	If the object is a drive (or a block device that is part of a drive), this is set to the value of the Drive:WWN property.
`drive.serial`	If the object is a drive (or a block device that is part of a drive), this is set to the value of the Drive:Serial property.
`drive.vendor`	If the object is a drive (or a block device that is part of a drive), this is set to the value of the Drive:Vendor property.
`drive.model`	If the object is a drive (or a block device that is part of a drive), this is set to the value of the Drive:Model property.
`drive.revision`	If the object is a drive (or a block device that is part of a drive), this is set to the value of the Drive:Revision property.
`drive.removable`	If the object is a drive (or a block device that is part of a drive), this is set to the string “true” only if the value of the Drive:Removable property is `TRUE`.
`drive.removable.bus`	If the object is a drive (or a block device that is part of a drive), this is set to the value of the Drive:ConnectionBus property. This variable is set only if the value of the Drive:Removable property is `TRUE`.
`drive.removable.media`	If the object is a drive (or a block device that is part of a drive), this is set to the value of the Drive:MediaCompatibility property. This variable is set only if the value of the Drive:Removable property is `TRUE`.
`id.type`	If the object is a block device, this property is set to the value of the Block:IdType property.
`id.usage`	If the object is a block device, this property is set to the value of the Block:IdUsage property.
`id.version`	If the object is a block device, this property is set to the value of the Block:IdVersion property.
`id.label`	If the object is a block device, this property is set to the value of the Block:IdLabel property.
`id.uuid`	If the object is a block device, this property is set to the value of the Block:IdUUID property.
`partition.number`	If the object is a partition, this property is set to the value of the Partition:Number property.
`partition.type`	If the object is a partition, this property is set to the value of the Partition:Type property.
`partition.flags`	If the object is a partition, this property is set to the value of the Partition:Flags property.

key	value
`partition.name`	If the object is a partition, this property is set to the value of the Partition:Name property.
`partition.uuid`	If the object is a partition, this property is set to the value of the Partition:UUID property.

For reference, the polkit actions defined by udisks 2.7.6 are included here:

```
<?xml version="1.0" encoding="utf-8"?>

<!DOCTYPE policyconfig PUBLIC
 "-//freedesktop//DTD PolicyKit Policy Configuration 1.0//EN"
 "http://www.freedesktop.org/standards/PolicyKit/1.0/policyconfig.dtd">

<policyconfig>
  <vendor>The Udisks Project</vendor>
  <vendor_url>https://github.com/storaged-project/udisks</vendor_url>
  <icon_name>drive-removable-media</icon_name>

  <!-- ###################################################################### -->
  <!-- Mounting filesystems -->

  <action id="org.freedesktop.udisks2.filesystem-mount">
    <_description>Mount a filesystem</_description>
    <_message>Authentication is required to mount the filesystem</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>yes</allow_active>
    </defaults>
  </action>

  <!-- mount a device considered a "system device" -->
  <action id="org.freedesktop.udisks2.filesystem-mount-system">
    <_description>Mount a filesystem on a system device</_description>
    <_message>Authentication is required to mount the filesystem</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>auth_admin_keep</allow_active>
    </defaults>
  </action>

  <!-- mount a device attached to another seat -->
  <action id="org.freedesktop.udisks2.filesystem-mount-other-seat">
    <_description>Mount a filesystem from a device plugged into another seat</_description>
    <_message>Authentication is required to mount the filesystem</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>auth_admin_keep</allow_active>
    </defaults>
  </action>

  <!-- mount a device referenced in the /etc/fstab file with the x-udisks-auth option -->
  <action id="org.freedesktop.udisks2.filesystem-fstab">
    <_description>Mount/unmount filesystems defined in the fstab file with the x-udisks-auth option</_description>
    <_message>Authentication is required to mount/unmount the filesystem</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>auth_admin_keep</allow_active>
    </defaults>
  </action>

  <!-- ###################################################################### -->
  <!-- Unmounting filesystems -->

  <!-- unmount a filesystem mounted by another user -->
  <action id="org.freedesktop.udisks2.filesystem-unmount-others">
    <_description>Unmount a device mounted by another user</_description>
    <_message>Authentication is required to unmount a filesystem mounted by another user</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>auth_admin_keep</allow_active>
    </defaults>
  </action>

  <!-- ###################################################################### -->
  <!-- Taking ownership of filesystems -->
```

```
<action id="org.freedesktop.udisks2.filesystem-take-ownership">
  <_description>Take ownership of a filesystem</_description>
  <_message>Authentication is required to take ownership of a filesystem.</_message>
  <defaults>
    <allow_any>auth_admin</allow_any>
    <allow_inactive>auth_admin</allow_inactive>
    <allow_active>auth_admin_keep</allow_active>
  </defaults>
</action>

<!-- ###################################################################### -->
<!-- Unlocking encrypted devices -->

<action id="org.freedesktop.udisks2.encrypted-unlock">
  <_description>Unlock an encrypted device</_description>
  <_message>Authentication is required to unlock an encrypted device</_message>
  <defaults>
    <allow_any>auth_admin</allow_any>
    <allow_inactive>auth_admin</allow_inactive>
    <allow_active>yes</allow_active>
  </defaults>
</action>

<!-- unlock a device considered a "system device" -->
<action id="org.freedesktop.udisks2.encrypted-unlock-system">
  <_description>Unlock an encrypted system device</_description>
  <_message>Authentication is required to unlock an encrypted device</_message>
  <defaults>
    <allow_any>auth_admin</allow_any>
    <allow_inactive>auth_admin</allow_inactive>
    <allow_active>auth_admin_keep</allow_active>
  </defaults>
</action>

<!-- mount a device attached to another seat -->
<action id="org.freedesktop.udisks2.encrypted-unlock-other-seat">
  <_description>Unlock an encrypted device plugged into another seat</_description>
  <_message>Authentication is required to unlock an encrypted device</_message>
  <defaults>
    <allow_any>auth_admin</allow_any>
```

```
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>auth_admin_keep</allow_active>
    </defaults>
  </action>

  <!-- unlock a device referenced in the /etc/crypttab file with the x-udisks-auth option -->
  <action id="org.freedesktop.udisks2.encrypted-unlock-crypttab">
    <_description>Unlock an encrypted device specified in the crypttab file with the x-udisks-auth option</_descrip
    <_message>Authentication is required to unlock an encrypted device</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>auth_admin_keep</allow_active>
    </defaults>
  </action>

  <!-- ###################################################################### -->
  <!-- Locking encrypted devices -->

  <!-- lock a device unlocked by another user -->
  <action id="org.freedesktop.udisks2.encrypted-lock-others">
    <_description>Lock an encrypted device unlocked by another user</_description>
    <_message>Authentication is required to lock an encrypted device unlocked by another user</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>auth_admin_keep</allow_active>
    </defaults>
  </action>

  <!-- ###################################################################### -->
  <!-- Changing passphrases on encrypted devices -->

  <action id="org.freedesktop.udisks2.encrypted-change-passphrase">
    <_description>Change passphrase for an encrypted device</_description>
    <_message>Authentication is required to change the passphrase for an encrypted device</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>yes</allow_active>
    </defaults>
  </action>

  <!-- change passphrase on a device considered a "system device" -->
  <action id="org.freedesktop.udisks2.encrypted-change-passphrase-system">
    <_description>Change passphrase for an encrypted device</_description>
    <_message>Authentication is required to change the passphrase for an encrypted device</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>auth_admin_keep</allow_active>
    </defaults>
  </action>

  <!-- ###################################################################### -->
  <!-- Setting up loop devices -->

  <action id="org.freedesktop.udisks2.loop-setup">
    <_description>Manage loop devices</_description>
    <_message>Authentication is required to set up a loop device</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <!-- NOTE: this is not a DoS because we are using /dev/loop-control -->
      <allow_active>yes</allow_active>
    </defaults>
  </action>

  <!-- ###################################################################### -->
  <!-- Deleting and modifying loop devices -->

  <action id="org.freedesktop.udisks2.loop-delete-others">
    <_description>Delete loop devices</_description>
    <_message>Authentication is required to delete a loop device set up by another user</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>auth_admin_keep</allow_active>
    </defaults>
  </action>

  <action id="org.freedesktop.udisks2.loop-modify-others">
```

```
    <_description>Modify loop devices</_description>
    <_message>Authentication is required to modify a loop device set up by another user</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>auth_admin_keep</allow_active>
    </defaults>
  </action>

  <!-- ###################################################################### -->
  <!-- Manage (start/stop) swapspace -->

  <action id="org.freedesktop.udisks2.manage-swapspace">
    <_description>Manage swapspace</_description>
    <_message>Authentication is required to manage swapspace</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>auth_admin_keep</allow_active>
    </defaults>
  </action>

  <!-- ###################################################################### -->
  <!-- Manage MD-RAID -->

  <action id="org.freedesktop.udisks2.manage-md-raid">
    <_description>Manage RAID arrays</_description>
    <_message>Authentication is required to manage RAID arrays</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>auth_admin_keep</allow_active>
    </defaults>
  </action>

  <!-- ###################################################################### -->
  <!-- Power off drives -->

  <action id="org.freedesktop.udisks2.power-off-drive">
    <_description>Power off drive</_description>
    <_message>Authentication is required to power off a drive</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>yes</allow_active>
    </defaults>
  </action>

  <!-- Power off a drive considered a "system device" -->
  <action id="org.freedesktop.udisks2.power-off-drive-system">
    <_description>Power off a system drive</_description>
    <_message>Authentication is required to power off a drive</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>auth_admin_keep</allow_active>
    </defaults>
  </action>

  <!-- Power off a drive attached to another seat -->
  <action id="org.freedesktop.udisks2.power-off-drive-other-seat">
    <_description>Power off a drive attached to another seat</_description>
    <_message>Authentication is required to power off a drive plugged into another seat</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>auth_admin_keep</allow_active>
    </defaults>
  </action>

  <!-- ###################################################################### -->
  <!-- Eject media from a drive -->

  <action id="org.freedesktop.udisks2.eject-media">
    <_description>Eject media</_description>
    <_message>Authentication is required to eject media</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>yes</allow_active>
    </defaults>
  </action>
```

```
<!-- eject media from a drive considered a "system device" -->
<action id="org.freedesktop.udisks2.eject-media-system">
  <_description>Eject media from a system drive</_description>
  <_message>Authentication is required to eject media</_message>
  <defaults>
    <allow_any>auth_admin</allow_any>
    <allow_inactive>auth_admin</allow_inactive>
    <allow_active>auth_admin_keep</allow_active>
  </defaults>
</action>

<!-- eject media from a drive attached to another seat -->
<action id="org.freedesktop.udisks2.eject-media-other-seat">
  <_description>Eject media from a drive attached to another seat</_description>
  <_message>Authentication is required to eject media from a drive plugged into another seat</_message>
  <defaults>
    <allow_any>auth_admin</allow_any>
    <allow_inactive>auth_admin</allow_inactive>
    <allow_active>auth_admin_keep</allow_active>
  </defaults>
</action>

<!-- ###################################################################### -->
<!-- Modify a device (create new filesystem, partitioning, change FS label etc.) -->

<action id="org.freedesktop.udisks2.modify-device">
  <_description>Modify a device</_description>
  <_message>Authentication is required to modify a device</_message>
  <defaults>
    <allow_any>auth_admin</allow_any>
    <allow_inactive>auth_admin</allow_inactive>
    <allow_active>yes</allow_active>
  </defaults>
</action>

<!-- modify a device considered a "system device" -->
<action id="org.freedesktop.udisks2.modify-device-system">
  <_description>Modify a system device</_description>
  <_message>Authentication is required to modify a device</_message>
  <defaults>
```

```
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>auth_admin_keep</allow_active>
    </defaults>
  </action>

  <!-- modify a device attached to another seat -->
  <action id="org.freedesktop.udisks2.modify-device-other-seat">
    <_description>Modify a device</_description>
    <_message>Authentication is required to modify a device plugged into another seat</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>auth_admin_keep</allow_active>
    </defaults>
  </action>

  <!-- rescan a device -->
  <action id="org.freedesktop.udisks2.rescan">
    <_description>Rescan a device</_description>
    <_message>Authentication is required to rescan a device</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>yes</allow_active>
    </defaults>
  </action>

  <!-- ###################################################################### -->
  <!-- Open a device for reading (for creating / restoring disk images) -->

  <action id="org.freedesktop.udisks2.open-device">
    <_description>Open a device</_description>
    <_message>Authentication is required to open a device</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>auth_admin_keep</allow_active>
    </defaults>
  </action>
  <action id="org.freedesktop.udisks2.open-device-system">
    <_description>Open a system device</_description>
    <_message>Authentication is required to open a device</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>auth_admin_keep</allow_active>
    </defaults>
  </action>

  <!-- ###################################################################### -->
  <!-- Manage system-wide configuration files such as /etc/fstab or
       /etc/crypttab ... including files referenced by these files.

       IMPORTANT: It is not secure to automatically grant authority
       for this action to groups of users. Neither is it secure to
       to allow a process to retain the authorization (e.g. don't
       use the _keep variants).
  -->

  <action id="org.freedesktop.udisks2.modify-system-configuration">
    <_description>Modify system-wide configuration</_description>
    <_message>Authentication is required to modify system-wide configuration</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>auth_admin</allow_active>
    </defaults>
  </action>

  <!-- Get secrets from system-wide configuration files -->
  <action id="org.freedesktop.udisks2.read-system-configuration-secrets">
    <_description>Modify system-wide configuration</_description>
    <_message>Authentication is required to retrieve secrets from system-wide configuration</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>auth_admin</allow_active>
    </defaults>
  </action>
  <!-- ###################################################################### -->
  <!-- Drive configuration (Power Management, Acustics, etc.) -->

  <action id="org.freedesktop.udisks2.modify-drive-settings">
    <_description>Modify drive settings</_description>
    <_message>Authentication is required to modify drive settings</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>auth_admin_keep</allow_active>
    </defaults>
  </action>

  <!-- ###################################################################### -->
  <!-- ATA SMART -->

  <!-- Update/refresh SMART data -->
  <action id="org.freedesktop.udisks2.ata-smart-update">
    <_description>Update SMART data</_description>
    <_message>Authentication is required to update SMART data</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>yes</allow_active>
    </defaults>
  </action>

  <!-- Set SMART data from blob -->
  <action id="org.freedesktop.udisks2.ata-smart-simulate">
    <_description>Set SMART data from blob</_description>
    <_message>Authentication is required to set SMART data from blob</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>auth_admin_keep</allow_active>
    </defaults>
  </action>

  <!-- Start and abort SMART self-tests -->
  <action id="org.freedesktop.udisks2.ata-smart-selftest">
    <_description>Run SMART self-test</_description>
    <_message>Authentication is required to run a SMART self-test</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>auth_admin_keep</allow_active>
    </defaults>
  </action>

  <!-- Enable/Disable SMART -->
  <action id="org.freedesktop.udisks2.ata-smart-enable-disable">
    <_description>Enable/Disable SMART</_description>
    <_message>Authentication is required to enable/disable SMART</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>auth_admin_keep</allow_active>
    </defaults>
  </action>

  <!-- ###################################################################### -->
  <!-- ATA Power Management -->

  <!-- Check power state -->
  <action id="org.freedesktop.udisks2.ata-check-power">
    <_description>Check power state</_description>
    <_message>Authentication is required to check the power state</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>yes</allow_active>
    </defaults>
  </action>

  <!-- Send standby command / resume from standby -->
  <action id="org.freedesktop.udisks2.ata-standby">
    <_description>Send standby command</_description>
    <_message>Authentication is required to put a drive into standby mode</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>yes</allow_active>
    </defaults>
  </action>

  <!-- Send standby command / resume from standby to a drive considered a "system device" -->
  <action id="org.freedesktop.udisks2.ata-standby-system">
    <_description>Send standby command to a system drive</_description>
    <_message>Authentication is required to put a drive into standby mode</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>auth_admin_keep</allow_active>
    </defaults>
  </action>

  <!-- Send standby command  / resume from standby to a drive on another seat -->
  <action id="org.freedesktop.udisks2.ata-standby-other-seat">
    <_description>Send standby command to drive on other seat</_description>
    <_message>Authentication is required to put a drive into standby mode</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>auth_admin_keep</allow_active>
    </defaults>
  </action>

  <!-- ###################################################################### -->
  <!-- ATA Secure Erase -->

  <!-- Send SECURE ERASE UNIT command -->
  <action id="org.freedesktop.udisks2.ata-secure-erase">
    <_description>Securely erase a hard disk</_description>
    <_message>Authentication is required to securely erase a hard disk</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>auth_admin_keep</allow_active>
    </defaults>
  </action>

  <!-- ###################################################################### -->
  <!-- Canceling jobs -->
  <!-- Cancel own job -->
  <action id="org.freedesktop.udisks2.cancel-job">
    <_description>Cancel job</_description>
    <_message>Authentication is required to cancel a job</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>yes</allow_active>
    </defaults>
  </action>

  <!-- Cancel job initiated by other user -->
  <action id="org.freedesktop.udisks2.cancel-job-other-user">
    <_description>Cancel job started by another user</_description>
    <_message>Authentication is required to cancel a job started by another user</_message>
    <defaults>
      <allow_any>auth_admin</allow_any>
      <allow_inactive>auth_admin</allow_inactive>
      <allow_active>auth_admin_keep</allow_active>
    </defaults>
  </action>

</policyconfig>
```

Generated by GTK-Doc V1.27