

🔒 How To Setup Session Management & Recording On A Switchboard (Admin Guide)

Version 6.0

Applies to Platform: Switchboard 6.9.x

Last update: 18 Dec 2025

A new major feature for the Endian Switchboard in 6.9.x is a session management and recording feature was created to support advanced user/usergroup restrictions to endpoint resources (applications) including monitoring and auditing these session activities to provide for policy enforcement and compliance. The actual result of using this feature is that when a user logs in, any resources that require session approval will now allow the user to "request access" where the user then fills out a short form including time window of when they wish to access the resource. Once approved (by a user with approval permissions), the user can then login and connect to the resource to perform their job duty during the defined time window. If the session policy has recording enabled and the activity the user performed was supported for recording, then the activity is recorded by the Switchboard and made available to the users with appropriate session permissions.

Requirements

Before you begin you will need the following in order to complete this process:

1. An Endian Switchboard that is already [setup](#) and accessible on a public IP or FQDN.
2. An account with administrative access on the Endian Switchboard.



Warning

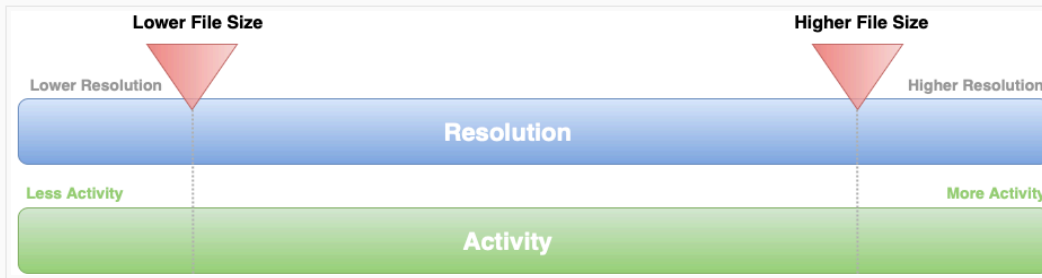
When recording is enabled on a session policy, the supported applications will be recorded in the appropriate manner. This feature is ONLY supported when using the Endian Switchboard Web Portal (not the Endian Connect App) for the following applications:

- RDP (video recording)
- VNC (video recording)

- SSH (video recording)

Recording Sizing Information

For each session recorded, a file is generated that consumes disk storage. Due to this, its important to understand the factors which can influence the size of the recorded session.



For video-based recordings (RDP & VNC), the main factors are as follows:

- Screen resolution – the higher the resolution the larger the recording size
- Screen activity – the more activity (e.g. window changes, movement, etc) the larger the recording size
- Session length – the longer the session the larger the recording size

For console recording (SSH & Telnet), the main factors are as follows:

- Session activity – the more activity (typing activity, multiplexing, I/O, etc) the larger the recording size
- Session length – the longer the session the larger the recording size

For reference purposes, here are some general estimations for various session recording sizes:

Application	Resolution / Activity	Recording Rate *	10 Minute File Size	1 Hour File Size
RDP	1024x768 / Moderate activity	~ 0.2–0.3 MB/min	2MB – 3MB	12MB – 18MB
RDP	1920x1080 / Moderate activity	~ 0.4–0.5 MB/min	4MB – 5MB	24MB – 30MB
SSH	Moderate activity **	~0.1 MB/min	1 MB	6 MB

* The recording rates and resulting file size estimations are based on testing calculations and can vary

** The moderate activity for SSH assumes started shell interaction and excludes multiplexing or heavy I/O

Manage User Permissions

There are three new user permissions introduced to support the new session management feature. They are outlined below:

- **Manage Session Policies:** The user can manage (create, edit, delete) session policies.
- **Approve Access Requests:** The user can approve session access requests. This user will automatically receive email notifications for new access requests for any user within their organization.

- **Manage Sessions:** The user can manage (view, join live or extend) sessions and view session history and recordings.

It's important to ensure you delegate these permissions appropriately based on your requirements.

You can find these permissions under *Switchboard > Users*.

Create Session Policy

A session policy is a policy that defines how access to a given resource (endpoint application) shall be granted – whether approval is required or not, recording settings, and other access constraints.

Navigate to *Switchboard > Sessions > Policies* and click the **New Policy** button.

The screenshot shows the Endian Switchboard interface. The left sidebar contains navigation options: Dashboard, Users, Devices, Applications, Messages, Sessions (highlighted), Sessions, Approvals, and Policies. The main content area is titled 'Policies' and contains a table of existing policies. A 'New policy' button is highlighted with a red box in the top right corner.

NAME	ORGANIZATION	APPROVAL	RECORDING	VPN	
approval and recording	endian	Required	● ■ ● ■	On	✍
recording only	endian	Not required	● ■ ● ■	On	✍
Root_Approval_Recording	Root Organization	Required	● ■ ● ■	Off	✍
Root_Approval	Root Organization	Required	● ■ ● ■	Off	✍
Root_Recording	Root Organization	Not required	● ■ ● ■	Off	✍

Here you can create a session policy by completing the form show below.

The screenshot shows the 'New policy' form in the Endian Switchboard interface. The form is titled 'New policy' and includes an 'Add' button in the top right corner. The form fields are numbered 1 through 5:

- NAME:** A text input field for the policy name.
- FOR ORGANIZATION:** A dropdown menu currently set to 'Root Organization'.
- Requires approval:** A checkbox with a label 'Requires approval' and a note: 'Enabling this feature will require all users/groups utilizing this session policy to request approval for all corresponding resources (gateways, endpoints, applications).'.
- PREFERENCES:** A section containing 'RECORDING' options: 'Video recording' and 'Text recording', both with checked checkboxes.
- CONNECTION OPTIONS:** A section containing 'Allow VPN connection via Connect App' with a checked checkbox.

An 'Add' button is located at the bottom of the form.

1. **Name:** Enter the descriptive name used for this session policy

2. **For Organization:** Here you can select the organization for which you wish to use this session policy.
3. **Requires approval:** Check this box to require approval prior to access being granted. If not selected, then the user will be able to access the endpoints without approval but session policy parameters will be applied and logged.
4. **Recording:** Here you can select which types of recording you wish to utilize. This **ONLY** applies to connections through the Endian Web Portal.
 - **Video Recording:** This will enable video recordings of RDP and VNC connections.
 - **Text Recording:** This will enable video (text) recordings of SSH and Telnet connections.
5. **Connection Options:** Check this box to allow users to connect to the endpoints using the Endian Connect App.
Remember, these sessions are not able to be recorded or monitored.

Click **Add** button to save the session policy.

Repeat this process to create as many session policies as needed.

Map Session Policy in ACAP

In order for the policy to be applied, it must match three specific variables: an Operator user, a specific endpoint and a specific application on that endpoint. This is achieved by using an [ACAP](#) (Advanced Action Policies) rule on the gateway that shields our endpoint. The standard ACAP syntax has been extended to allow for a fourth and optional value, the Policy name:

```
ALLOW "Application Name/domain" ON "endpoint_name" TO "username@email.address" WITH "Policy Name"
```

Note

For historical reasons, the only place where the domain name must be explicitly given in the ACAP rule, is in the first field, where you have to provide the unescaped Application name, followed by the domain path.

Note

The user cannot be a superuser and he must already have access to the gateway thanks to the standard Switchboard permissions, e.g. being at least a "regular user" of that gateway, or being at least "member" of a user group that has itself at least "regular user" access level on the gateway.

The ACAP policies are contained within the parameters of a Gateway device. To edit, you can click on *Switchboard > Devices > Gateways* and click the **Edit** button next to the desired gateway.

The screenshot shows the Endian Switchboard Virtual Appliance interface. On the left is a navigation menu with options: Dashboard, Users, Devices (highlighted), Gateways, Groups, and Applications. The main content area displays a table of gateways. The table has columns for Name, Organization, Description, Serial, Groups, Provisioning, and Actions. One gateway is listed: 'sparkling-sunset-8172' with description 'virtual-x64 6.0'. The 'Actions' column for this gateway contains several icons, with the 'Add gateway' icon (a plus sign) highlighted by a red box and a red arrow. Above the table are buttons for 'Plug & Connect (Autoregistration)', 'Add gateway', and 'Download CA certificate'. Below the table, there is a legend for the status icons and a pagination control showing 'Total 1, 20 items / page'.

Navigate to the Permissions tab and you will find the Policies section where you can create the ACAP rules. You can learn about the basic syntax and usage in this [article](#). We will build a sample ruleset below with an explanation for each item shown as a comment.

```
# Grant SSH access on the gateway to some power user
ALLOW "Secure Shell" ON "gateway" TO "poweruser@domain.org"

# Grant access (regulated by some policy) to an operator user
ALLOW "Secure Shell" ON "gateway" TO "operator@domain.org" WITH "Approve and record"

# Deny access to SSH to everyone else
DENY "Secure Shell" ON "gateway" TO *

# Grant policy regulated access to any other resource for a specific user group
ALLOW TO usergroup:Operations WITH "Record only"

# Deny access to every resource to anyone else
DENY
```

For this example, there would need to be two session policies: (1) named **Approve and record** and another (2) named **Record only**.

Click the **Add / Change** button to save the ACAP for this gateway. You can then repeat this process for each gateway required the use of session policies.

Once this is all completed, the policies should be applied to applicable users when they login and attempt to connect to protected resources identified in the policies.

endian user@endian.test

Switchboard Virtual Appliance
Version 6.8.6

Dashboard
Sessions

1/5 Online users
3/4 Online gateways
6 Endpoints
System info

Endpoint: gateway-edge-x/endian >> windows-11@gateway-edge-x/endian

Organization: endian
Virtual IP address: 100.100.0.17
Real IP address: 192.168.102.100
Status: Online
Connect

APPLICATION	TYPE	DESCRIPTION	APPROVAL	
Windows Remote Desktop	🖥️	Open a Windows Remote Desktop session (RDP)	● To request	Request access
Windows Remote Desktop	🖥️	Open a Windows Remote Desktop session (RDP)	● To request	Request access

points Filter...
status
online user connected
online user connected
1 - 1 of 1 gateways

Comments

