

---

## Manage Files and Folders

 For supported software information, click [here](#).

The rules that you configure for captive portal and for document fingerprinting and exact data match (EDM), which are part of data loss prevention (DLP), need to access files that are uploaded to the Director node. For captive portal, you can upload files that contain the text for a custom captive file page. For document fingerprinting and EDM, you can upload files that contain the custom data patterns to be matched.

In addition, for certificates, you can upload the files containing the certificate authority (CA) certificate, the CA chain, and the private key to the Director node.

You upload these files from your local system to the Director node. For certificate and EDM files, you upload them directly to the Director node. For fingerprint files, you first create folders (directories) to contain the files to be fingerprinted and then you upload the files. Before you upload the files, you select the organization that contains the Versa Operating System™ (VOS™) devices that need to access the uploaded files. To push the uploaded files to the organization's appliances, you need to commit the revised template to the VOS devices.

This article describes how to upload files for captive portal, document fingerprinting, EDM, and certificates, and how to create and manage folders for these files.

---

## Enable File Transfer

Before you can upload and manage files, you must enable file transfer on the VOS device. To do this, go to the shell on the Director node, and then issue the following commands to check whether the SECURITY\_FILE\_TRANSFERS parameter vnms.properties file is set to true:

```
admin@Director$ grep SECURITY_FILE_TRANSFERS /opt/versa/vnms/etc/conf/vnms.properties
SECURITY_FILE_TRANSFERS=true

admin@Director$ grep SECURITY_FILE_TRANSFERS /var/versa/vnms/data/conf/vnms.properties
SECURITY_FILE_TRANSFERS=true
```

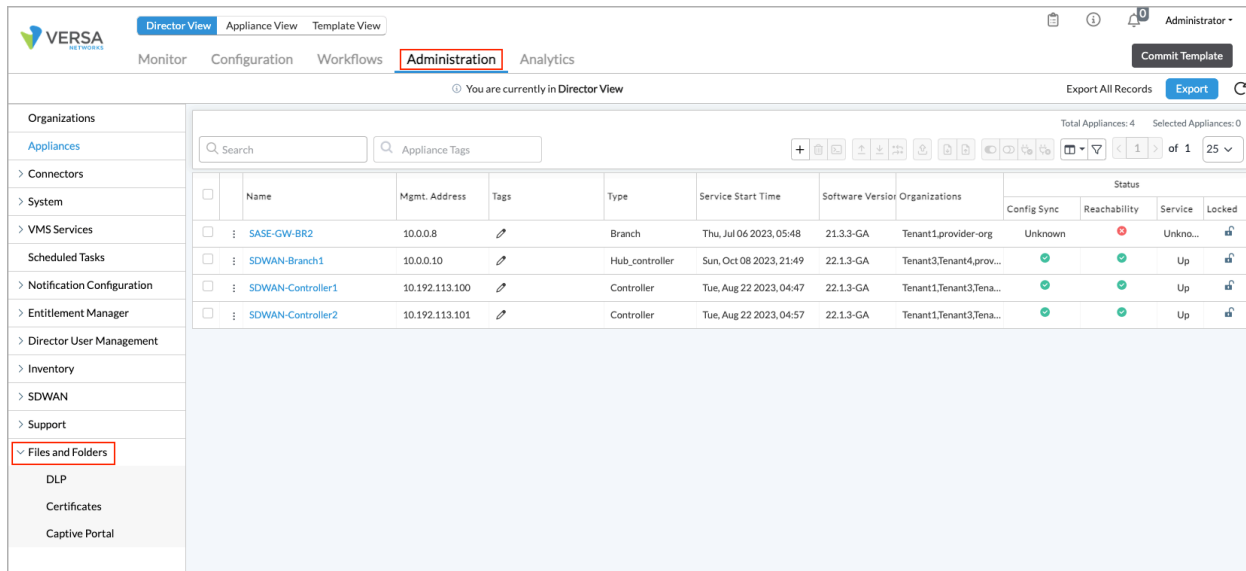
If the output shows that SECURITY\_FILE\_TRANSFERS=false in either of the files, edit the file and set SECURITY\_FILE\_TRANSFERS=true.

---

## Manage Files and Folders

To manage files and folders:

1. In Director view, select the Administration tab in the top menu bar.
2. Select Files and Folders in the left menu bar. The left menu bar shows three categories: DLP, Certificates, and Captive Portal.



---

## Manage DLP EDM and Fingerprinting Files and Folders

For DLP, you can upload files that are used by EDM and document fingerprinting into a folder named DLP, and you can create and manage the folders in which these files are stored.

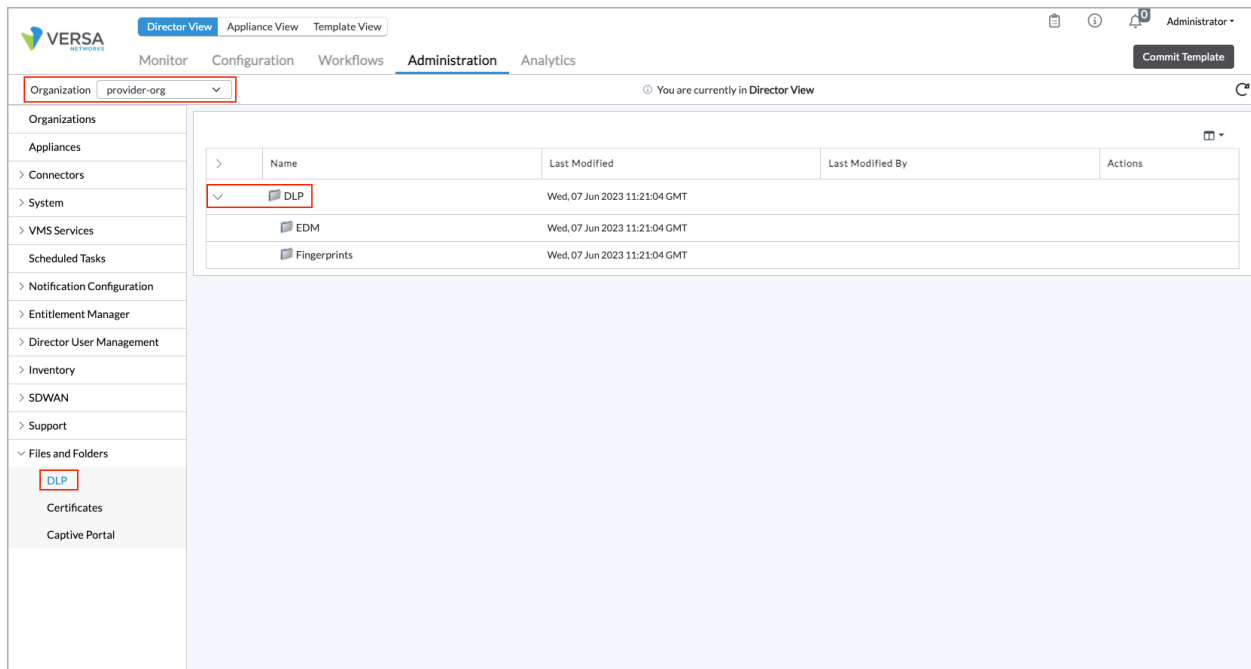
The DLP folder contains two folders: EDM and Fingerprints.

For the EDM folder, you can upload files directly into the folder, but you cannot create new subfolders in it.

For the Fingerprint folder, you must first create a subfolder, and then you can upload files into the subfolder.

To manage the files and folders for EDM and document fingerprinting:

1. In Director view, select the Administration tab in the top menu bar.
2. In the Organization field, select the organization that contains the VOS devices that need to access the uploaded files.
3. Select Files and Folders > DLP in the left menu bar. The following screen displays.



4. Click the ➤ Expand icon to the left of the DLP folder to display the folders in the DLP folder.

5. To upload files for EDM processing:

a. Highlight the EDM row, and then click the Add Files icon in the Action column.

b. In the Add File popup window, enter information for the following fields.

Field	Description
Choose File	Click to upload from your local system. The file must be in CSV format.
Enable Hashing	Click to hash the file that is being uploading using the SHA-256 algorithm. Hash the file using any one-way hash utility tool before uploading it.  <i>Default: Enabled</i>

6. To upload files for document fingerprinting:

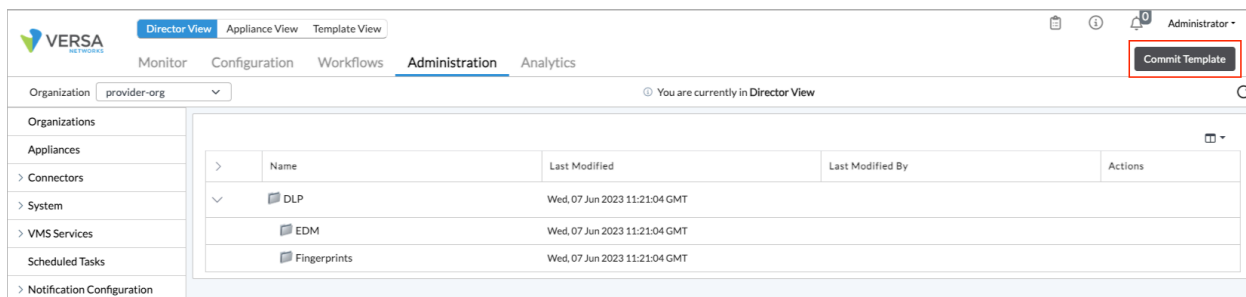
a. Highlight the Fingerprints row, and then click the Add Folders icon in the Action column.

b. In the Add Folders popup window, enter a name for the new folder, and then click OK to create the new folder.

- c. Highlight the new folder, and then click the Add Files icon in the Action column.
- d. In the Add File popup window, enter information for the following fields.

Field	Description
Choose File	Click to upload from your local system. The file must be in CSV format.
Enable Hashing	Click to hash the file that is being uploading using the SHA-256 algorithm. Hash the file using any one-way hash utility tool before uploading it.  <i>Default: Enabled</i>

7. After you have uploaded the files, click the Commit Template button to push the template configuration to the devices.



## Manage Certificate Files and Folders

For certificates, you can upload the files containing the C certificate, the CA chain, and the private key.

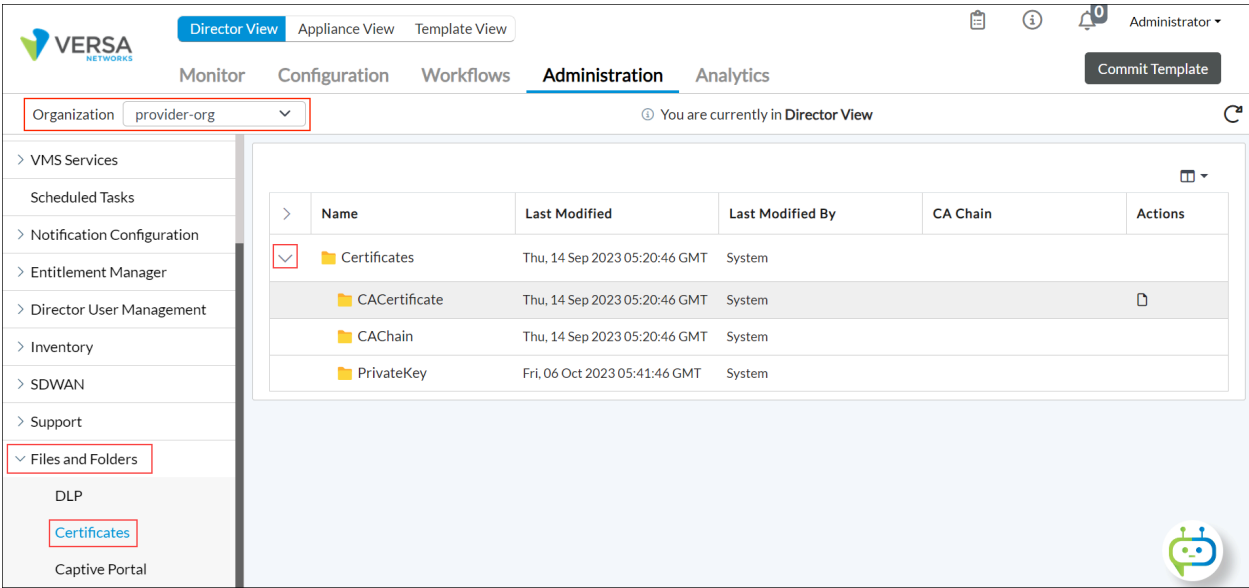
A certificate authority is a trusted entity that issues a CA certificate, which verifies a digital entity's identity on the internet. A private key is required to access secured traffic using a certificate. To secure the traffic on a VOS device, you can use either a self-signed CA certificate or a trusted CA certificate. A certificate chain is an ordered list of certificates, containing an SSL/TLS certificate and CA certificates, that allow the receiver to verify that the sender and all CA's are trustworthy.

You upload files that are used for certificates into three folders: CA Certificate, CA Chain, and Private Key

To upload certificate files and to manage the certificate folders:

1. In Director view, select the Administration tab in the top menu bar.
2. In the Organization field, select the organization that contains the VOS devices that need to access the uploaded files.

3. Select Files and Folders > Certificates in the left menu bar. The following screen displays.



4. Click the ➤ Expand icon to the left of Certificates to display the default subfolder in the Certificates folder.
5. To upload a CA certificate, select the CA Certificate row, and then click the Add Files icon in the Actions column. In the Add File popup window, enter information for the following fields.

Add File

×

Upload File (Note - Allowed file formats are .zip) \*

Choose File

No file chosen

Name

Pass Phrase

CA Chain


---Please Select---

▼

OK

Cancel

Field	Description
Choose File	Click to upload a CA certificate file from your local system. The CA certificate file must be in .zip format.
Name	Enter a name for the CA certificate file.
Pass Phrase	Enter a password. It can be up to 63 characters.
CA Chain	Select a CA chain.

- Click OK.
- To upload a CA chain, select the CA Chain row, and then click the  Add Files icon in the Actions column. In the Add Files popup window, enter information for the following fields.

Add File

Upload File (Note - Allowed file formats are .crt, .cer or .pem)

Choose File


No file chosen

Name

OK

Cancel

Field	Description
Choose File	Click to upload a CA chain file from your local system. The file must be in .cer, .crt, or .pem format.
Name	Enter a name for the CA chain file.

- Click OK.
- To upload a private key, select the Private Key row, and then click the  Add Files icon in the Actions column. In the Add Files popup window, enter information for the following fields. Note that private key files must be in .key or .pem format.

Add File

Upload File (Note - Allowed file formats are .key or .pem)

Choose File

No file chosen

Name \*

Pass Phrase

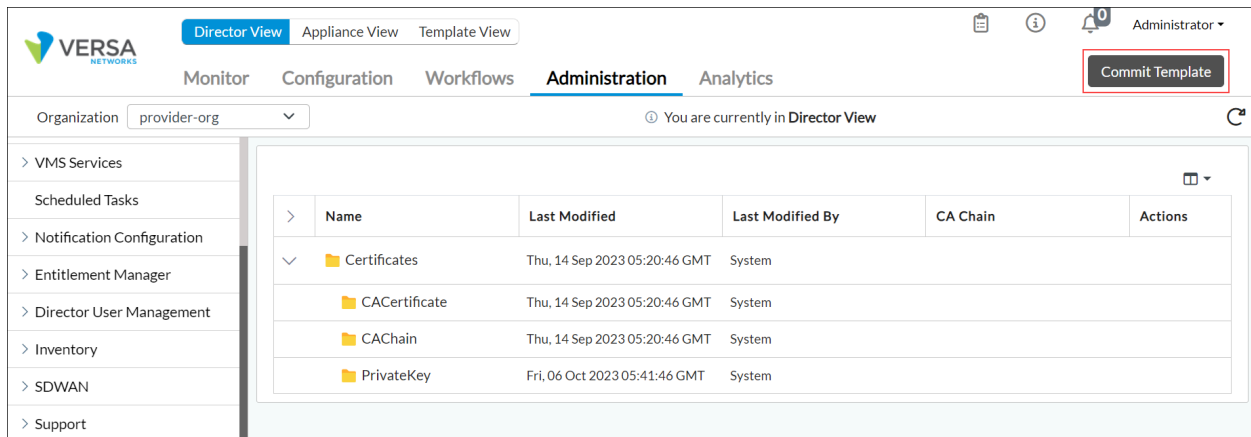
OK

Cancel

Field	Description
Choose File	Click to upload a private key file from the local system. The file must be in .key or .pem format.
Name (Required)	Enter a name for the private key file.
Pass Phrase	Enter a password. It can be up to 63 characters.

- After you have uploaded the certificate files, click the Commit Template button to push the template configuration to the devices.



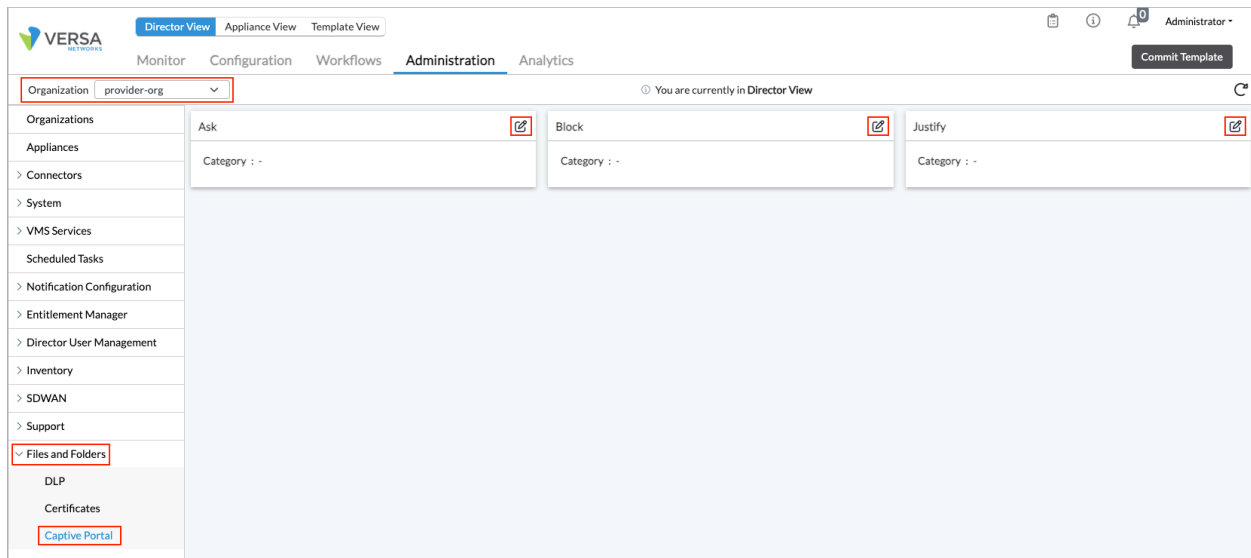



## Manage Captive Portal Files and Folders

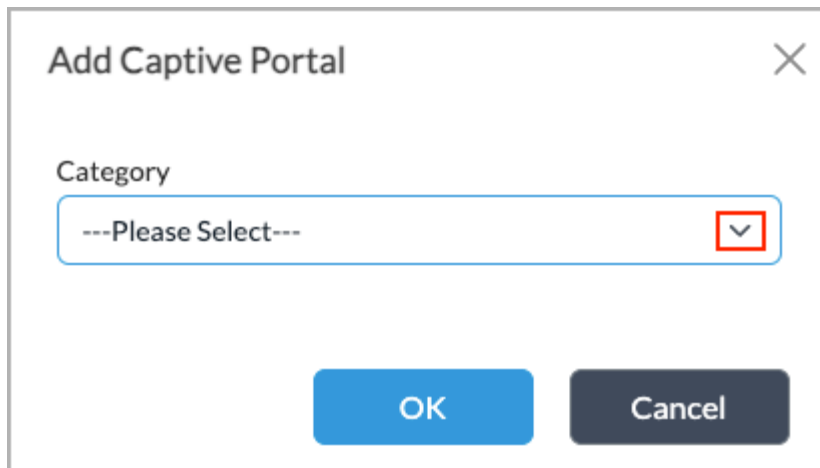
You can upload files to associate with the Ask, Block, and Justify captive portal actions. You can upload different files for each action.

To manage files and folders for captive portal:

1. In Director view, select the Administration tab in the top menu bar.
2. In the Organization field, select the organization that contains the VOS devices that need to access the uploaded files.
3. Select Files and Filters > Captive Portal in the left menu bar. The following screen displays.

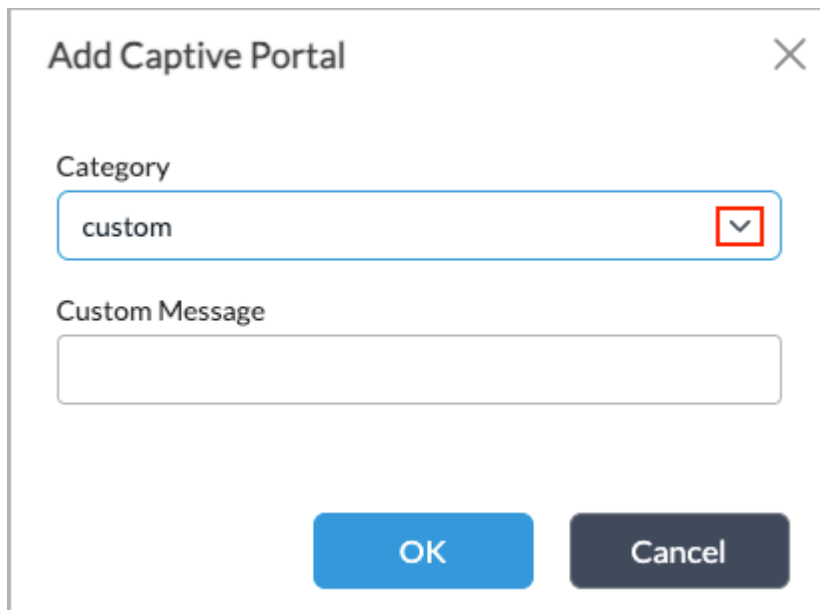


4. To configure a captive portal category for the Ask, Block, or Justify action, click the  Edit icon in the Ask, Block, or Justify box. In the Add Captive Portal popup window, select Ask, Block, or Justify in the Category field.



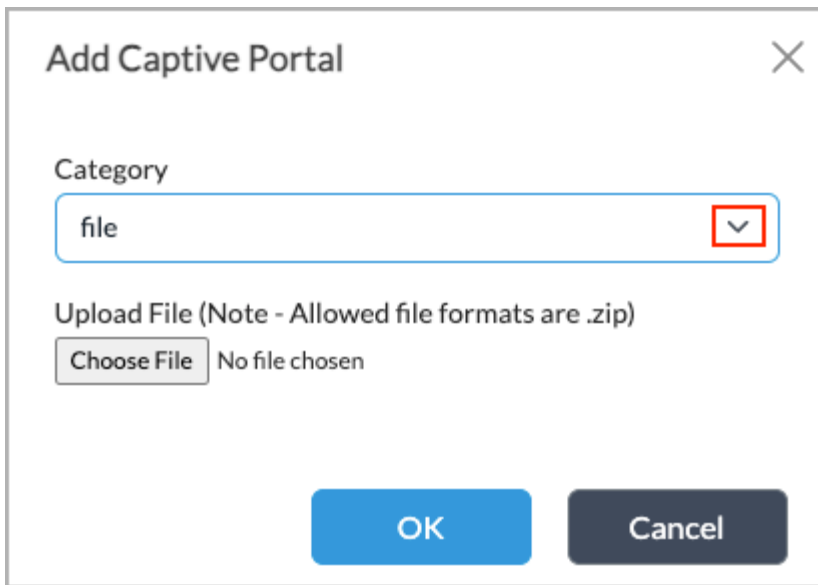
The dialog box is titled "Add Captive Portal" and has a close button (X) in the top right corner. It contains a "Category" label above a dropdown menu. The dropdown menu currently shows "---Please Select---" and has a red square highlighting the downward arrow. At the bottom, there are two buttons: "OK" (blue) and "Cancel" (dark grey).

5. In the Category field, select a category.
  - a. If you select Default, click OK.
  - b. If you select Custom, the following screen displays. Enter a custom message, and then click OK.



The dialog box is titled "Add Captive Portal" and has a close button (X) in the top right corner. It contains a "Category" label above a dropdown menu. The dropdown menu now shows "custom" and has a red square highlighting the downward arrow. Below the dropdown is a "Custom Message" label above a text input field. At the bottom, there are two buttons: "OK" (blue) and "Cancel" (dark grey).

- c. If you select File, the following screen displays. Click Choose File to upload a captive portal file in .zip format from your local system, and then click OK.



**Add Captive Portal** [X]

Category

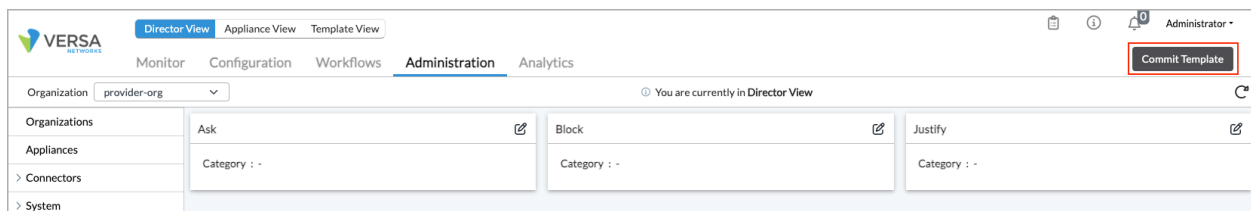
file [v]

Upload File (Note - Allowed file formats are .zip)

Choose File No file chosen

OK Cancel

- After you have uploaded the captive portal files, click the Commit Template button to push the template configuration to the devices.



## Supported Software Information

Releases 22.1.3 and later support all content described in this article.

## Additional Information

[Configure CA Certificates and CA Chains](#)

[Configure URL Filtering](#)