



## Monitoring VNF Using D-MONA

---

- [Onboarding D-MONA, on page 1](#)
- [Deploying D-MONA, on page 1](#)
- [Configuring D-MONA, on page 2](#)
- [Deploying VNF Using D-MONA, on page 2](#)
- [Monitoring Using D-MONA, on page 3](#)

## Onboarding D-MONA

ETSI NFV MANO supports Distributed Monitoring and Actions (D-MONA) for effective monitoring of the VNFs. D-MONA is a standalone monitoring application. For more information, see [Monitoring VNFs Using D-MONA in the Cisco Elastic Services Controller User Guide](#).

To onboard D-MONA, you must fulfill the prerequisites and prepare the deployment data model:

### Prerequisites

- Ensure connectivity between ESC and D-MONA.
- Ensure connectivity between D-MONA and the deployed VNFs.
- Only ESC Active/Active deployment is supported by D-MONA.

For information on deploying D-MONA, see [Deploying D-MONA, on page 1](#).

## Deploying D-MONA

ESC supports 1:1 D-MONA deployment for a VIM. A single D-MONA instance monitors VNF on a single VIM.

For using D-MONA in your infrastructure, you must:

1. Deploy the D-MONA with the monitoring infrastructure.
2. Deploy the VNFs using the D-MONA for monitoring their respective liveness.

After deployment, D-MONA is monitored by the local MONA running on the ESC VM.

For information on deploying VNFs using D-MONA, see [Deploying VNF Using D-MONA, on page 2](#).

## Configuring D-MONA

D-MONA reuses the ESC 5.0 image. You can view two types of runtime behavior; one from a typical ESC deployment, and the other one with capabilities provided by D-MONA.

### D-MONA Day Zero Configuration

The D-MONA runtime behavior is controlled by the day 0 configuration provided to the VM at the time of deployment.

The following example shows D-MONA SSH access configuration:

```
<configuration>
  <dst>--user-data</dst>
  <file>file:///opt/cisco/esc/esc-config/dmona/iser-data.template</file>
  <variable>
    <name>vm_credentials</name>
    <val>REPLACED_WITH_GENERATED_PWD</val>
  </variable>
</configuration>
```

The `vm_credentials` passes the encrypted password to admin for SSH access to D-MONA.

The following example shows the D-MONA ESC certificate configuration:

```
<configuration>
  <dst>/opt/cisco/esc/moan/dmona.crt</dst>
  <data>$DMONA_CERT</data>
</configuration>
```

For monitoring using D-MONA, see [Monitoring Using D-MONA, on page 3](#).

## Deploying VNF Using D-MONA

For deploying the VNFs using D-MONA for monitoring, you must have the D-MONA with the `monitoring.agent.vim.mapping day-0` variable set to true within the same `vim_connector`. When ESC detects D-MONA, monitoring of the VNF is assigned to that D-MONA, otherwise the local MONA handles the monitoring.

The following example shows the D-MONA VNFD:

```
tosca_definitions_version: tosca_simple_yaml_1_2
description: D-MONA VNFD (SOL001 v0.10.0)

imports:
  - cisco_nfv_sol001_types.yaml
  - etsi_nfv_sol001_vnfd_0_10_0_types.yaml

metadata:
  template_name: D-MONA
  template_author: Cisco Systems
  template_version: '1.0'

dsl_definitions:
  descriptor_id: &descriptor_id f5b37b47-d9bd-4605-afb0-30c0d659a3c2
  provider: &provider cisco
  product_name: &product_name D-MONA
```

```

software_version: &software_version '1.0'
descriptor_version: &descriptor_version '1.0'
flavour_id: &flavour_id default
flavour_description: &flavour_description 'Default VNF Deployment Flavour'
vnfm: &vnfm '9:Cisco Elastic Services Controller:v04.04.01'

```

## Monitoring Using D-MONA

To monitor the VNFs using D-MONA, you must deploy the ETSI VNFD D-MONA and then deploy the ETSI VNFD monitored by D-MONA. For information on deploying D-MONA, see [Deploying VNF Using D-MONA, on page 2](#).

The D-MONA parameters are defined within the VNFD, or provided as additionalparams in the instantiate D-MONA VNF payload.

An ETSI compliant VNFD is used for the deployment of D-MONA.

The input parameters, KPI data, and config paramters are required for instantiation of D-MONA deployment.

The input parameters are either defined within the VNFD or provided as additionalParams section of instantiate D-MONA VNF payload.

**Table 1: Input Parameters for D-MONA Deployment**

Parameter	Description
SW_IMAGE_NAME	The name of ESC image
DMONA_CERT	The HTTPS certificate
DMONA_AGENT_ID	The URL or ID of the monitoring agent that will monitor the VM
ADMIN_PASSWORD	The admin user password
SECURITY_BASIC_ENABLED	A flag that indicates whether basic security is enabled or not
SECURITY_USER_NAME	A security user to communicate with ESCManager
SECURITY_USER_PASSWORD	A security user's password used to communicate with ESCManager

KPI data:

- monitoring\_agent—value defined for DMONA\_AGENT\_ID in the input parameter.
- property\_list
  - name—protocol
  - value—https
  - name—port
  - value—8443

- name—path
- value—mona/v1/health/status

Config data parameters:

- user-data.txt
  - admin\_password—value defined for ADMIN\_PASSWORD in input parameter
- application—dmona.template
  - monitoring.agent—true
  - security\_basic\_enabled—value defined for SECURITY\_BASIC\_ENABLED in input parameter
  - security\_user\_name—value defined for SECURITY\_USER\_NAME in input parameter
  - security\_user\_password—value defined for SECURITY\_USER\_PASSWORD in input parameter
  - monitoring.agent.vim.mapping—true

Example payload:

```
config_data:
  '--user-data':
    file: ../Files/Scripts/user-data.txt
    variables:
      admin_password: { get_input: ADMIN_PASSWORD }
  '/opt/cisco/esc/mona/dmona.crt':
    data: { get_input: DMONA_CERT }
  '/opt/cisco/esc/mona/config/application-dmona.properties':
    file: ../Files/Scripts/application-dmona.template
    variables:
      monitoring.agent: true
      security_basic_enabled: { get_input: SECURITY_BASIC_ENABLED }
      security_user_name: { get_input: SECURITY_USER_NAME }
      security_user_password: { get_input: SECURITY_USER_PASSWORD }
      monitoring.agent.vim.mapping: true
```