Turbonomic 7.17.5 Installation Guide

Turbonomic, Inc

500 Boylston St, 7th floor
Boston, MA 02116 USA
Phone: (844) 438-8872
www.turbonomic.com

COPYRIGHT

END-USER LICENSE AGREEMENT

https://cdn.turbonomic.com/wp-content/uploads/Turbonomic_Click_Through_Customer-License.pdf

Contents

Introduction

Thank you for choosing Turbonomic, the Intelligent Workload Management solution for Cloud and Virtualized Environments. This guide gives you information you need to install Turbonomic in your virtual environment, install your license, and get started managing your resources.

If you have any questions, please see our support site at `https://support.turbonomic.com`.

Sincerely:

The Turbonomic Team

Minimum Requirements

The requirements for running a Turbonomic instance depend on the size of the environment you are managing. Turbonomic keeps a real-time representation of your environment in memory. The greater the number of entities to manage, and the greater the relationships between them, the more resources you need for the VM that runs Turbonomic. And as the VM requirements increase, so do the requirements for the physical machine that hosts the VM.

The requirements listed here are recommendations that you should keep in mind as you plan your Turbonomic deployment. The minimum memory requirement is 64 GB. After deploying, if you find that you need to change memory capacity, CPU capacity, or both for the VM, you can shut it down, make changes, and then power it up again to use the new capacity.

In most cases you can run Turbonomic on a host that meets the following minimum requirements:

Supported Hypervisors		Storage Requirements	Memory	CPUs
VMware	vCenter versions 5.5, 6.0, 6.5, and 6.7	1.25 TB or greater. **NOTE:** Can be thin provisioned depending on the storage requirements.	64 GB	8 vCPUs

Turbonomic provides an OVA file which is preconfigured with two hard drives. A minumum of 1.25 TB is necessary to ensure that the drives have the proper amount of space for storage.

Turbonomic requires a browser capable of displaying HTML5 pages.

Turbonomic requires static IP addressing.

Installing Turbonomic

As you get started with Turbonomic, please note that for this release the only supported hypervisor for installation is vCenter.

Installing on VMware Systems

This download of the Turbonomic instance is in the `.OVA 1.0` format.

To install Turbonomic:

1. Download the Turbonomic installation package.

   The email you received from Turbonomic includes links to the Turbonomic download pages. You can get the installation package from there.

   The installation package includes the `turbonomic_t8c-<version>-<XXXXXXXXXXXXXX>.ova` file

   where <version> is the Turbonomic version number and <XXXXXXXXXXXXXX> is the timestamp.

   For example: `turbonomic-t8c-7.17.3-20190916164429000.ova`

   The OVA file deploys as a VM with the Turbonomic components already installed.

2. Import the OVA file into your datacenter.

   Use the vCenter Server client to import the OVA into your environment.

3. Deploy the Turbonomic VM.

   Create the VM using the OVA file. Ensure that the physical machine hosting the VM meets the minimum requirements (see Minimum Requirements *(page 5)*).

   Manually modify the default values for CPU and Memory:

   a. Right-click the VM and choose **Edit Settings**.

   b. Type **8** for CPU.

c. Type **64** for Memory.

d. Click **OK** to save the settings

e. Power on the VM.

4. Open the remote console.

   For the Turbonomic VM that you just deployed:

   a. Choose the **Summary** tab.

   b. Click **Launch Remote Console**.

5. Set up the Turbonomic System Administrator account.

   a. In the remote console, log in with the following default credentials:

      - Username: `turbo`

        Do not use the account name, `root`.

      - Password: `vmturbo`

        Then, you will be prompted to enter a new password.

   b. Enter your new password.

      The new password must comply with the strong password policy (a mixture of upper- and lower-case letters, numbers, and a symbol). Only you will know this new password.

      > **NOTE:**
      > *Be sure to save the turbo account credentials in a safe place.* For security reasons, this is the only account that can access and configure the Turbonomic VM.

   c. Enter your new password again to verify it.

6. Set up the static IP address.

   a. In the remote console, start the NetworkManager user interface.

      Type: `sudo nmtui`

   b. Edit the `eth0 ethernet` connection.

      Use the arrow keys to navigate in NetworkManager.

      In NetworkManager, choose the `Edit` option and click <OK> to open the Edit Connection dialog box.

      Then, choose `Ethernet` from the list of options and fill out the following information (values given are examples only).

      - Profile Name: `System eth0`
      - Device: `eth0`

      Next, expand `IPv4 CONFIGURATION` and fill out the configuration subsettings based on your environment:

      - IPv4 Configuration: `<Manual>`

- Addresses: Specify the static IP address you want, with the subnet mask on the same line. For example:

  `10.0.254.10/24`

- Gateway, DNS Servers, and Search domains: Give values that are valid for your network environment.

When you are satisfied with your settings, click <OK> and <Back> to return to the configuration list. Verify that the connection you just created is present.

c. Exit NetworkManager.

Click <Quit> to return to the command line.

7. Restart the network service in the Turbonomic VM.

Type: `sudo systemctl restart network`

8. Deploy Turbonomic Kubernetes nodes.

When you deploy Turbonomic on Kubernetes, you deploy one Kubernetes node as a VM that will host pods to run the Turbonomic components. The script to deploy and initialize the Kubernetes node also deploys the Kubernetes pods that make up the Turbonomic application.

Start a secure session (SSH) on your Turbonomic VM as the turbo user and perform the following steps:

a. Initialize the Kubernetes node and deploy the pods.

Execute the script: `/opt/local/bin/t8c.sh`

Do not specify `sudo` when you execute this script.

The script should take up to 20 minutes to complete.

b. Verify that the the deployment succeeded.

At the end of the script output, in the summary section, verify that no errors are reported. If any errors are reported, contact Turbonomic Support.

c. Verify that the Turbonomic application installed correctly.

To verify the installation of the application, execute the command:

```
kubectl get pods -n turbonomic
```

After all of the pods start up, the READY column should read `1/1` and the STATUS column should read `Running`.

You should see output similar to the following:

```
NAME                                        READY   STATUS    RESTARTS
action-orchestrator-b6454c9c8-mfl85         1/1     Running   0
api-7887c66f4b-shndq                        1/1     Running   0
arangodb-7f646fc5fc-zhcwf                   1/1     Running   0
auth-5b86976bc8-vxwz4                       1/1     Running   0
clustermgr-85548678d9-r5wb8                 1/1     Running   0
consul-7f684d8cb8-6r677                     1/1     Running   0
cost-5f46dd66c4-6d6cb                       1/1     Running   0
group-5bfdfbc6f8-96bsp                      1/1     Running   0
history-5fc7fbc855-6zslq                    1/1     Running   0
kafka-74cc77db94-dfrbl                      1/1     Running   0
market-5f54699447-z4wkm                     1/1     Running   0
mediation-actionscript-57b4fc6df-4lzfv      1/1     Running   0
```

```
mediation-appdynamics-6d65f8766f-kb44l       1/1     Running   0
mediation-hpe3par-d7c475c4c-v8ftc            1/1     Running   0
mediation-hyperv-6bd8c94df5-4dbzx            1/1     Running   0
mediation-netapp-7f8fc955d9-4kkdl            1/1     Running   0
mediation-oneview-7dbd7b54cf-7rfqp           1/1     Running   0
mediation-pure-58c4bd8cd9-8n256              1/1     Running   0
mediation-ucs-6f4bb9889-9rnqk                1/1     Running   0
mediation-vcenter-5bc4f5fbd4-nzm4j           1/1     Running   0
mediation-vcenterbrowsing-5c5987f66c-bfjq4   1/1     Running   0
mediation-vmax-6c59969b89-28t9j              1/1     Running   0
mediation-vmm-9c4878cf9-rfxnl                1/1     Running   0
nginx-5b775f498-sm2mm                        1/1     Running   0
plan-orchestrator-6dffc4c9b6-p5t5n           1/1     Running   0
reporting-b44fbdfb4-8fjv5                    1/1     Running   0
repository-6d555bb4bf-fxldh                  1/1     Running   0
rsyslog-fd694878c-5tb2c                      1/1     Running   0
t8c-operator-558bcc758d-5h8mp                1/1     Running   0
topology-processor-b646b786b-9skp7           1/1     Running   0
zookeeper-5f65b5bf69-nnmbt                   1/1     Running   0
```

d. Verify that the Load Balancer has installed correctly.

To verify the presence of the Load Balancer, execute the command:

```
kubectl get services -n turbonomic|grep LoadBalancer
```

You should see output similar to the following:

```
nginx  LoadBalancer   10.10.10.10   10.10.10.11  443:32669/TCP,80:32716/TCP  17h
```

e. Enable mediation.

The t8c.sh script automatically enables mediation. No user action is required.

For Turbonomic to manage your IT environment, it must attach to targets in your environment so it can perform discovery and execute actions. The combination of the processes of discovery and action execution is *mediation*. This release of Turbonomic on Kubernetes supports mediation through the following targets. If you need to use additional targets that are not in this list, contact Turbonomic Support.

- Hypervisors
  - VMware vCenter 5.1, 5.5, 6.0, 6.5, and 6.7
  - Microsoft Hyper-V 2008 R2, Hyper-V 2012, and Hyper-V 2012 R2
- Fabric Managers
  - Cisco UCS 3.1+
  - HPE OneView 3.00.04+
- Guest OS Processes
  - AppDynamics 4.1+

- Storage Managers
  - NetApp Cmode/7mode using ONTAP 8.0+ (excluding AFF and SolidFire)
  - EMC VMAX using SMI-S 8.1+
  - Pure Storage F-series and M-series arrays
  - HP 3PAR InForm OS 3.2.2+, 3PAR SMI-S, 3PAR WSAPI
- Cloud Managers
  - Microsoft System Center 2012 Virtual Machine Manager and System Center 2012 R2 Virtual Machine Manager

For information about these targets, see the *Turbonomic Target Configuration Guide*.

9. Log in to the Turbonomic user interface and set the administrator user account password.

   After the components start up, in your Web browser, type the static IP address of your Turbonomic VM. Your browser redirects to `https://[MyIPAddress]/app/index.html#/authentication/login`. This is the login page for Turbonomic users.

   Turbonomic includes a default user account named `administrator`. You cannot delete this account, and you must set your own password for it.

   In the login page, enter the information as required, and make a note of it.

   - Use the default credential for **USERNAME**: `administrator`.
   - Type a password for **PASSWORD**.

     The new password must comply with the strong password policy (a mixture of upper- and lower-case letters, numbers, and a symbol). Only you will know this new password.
   - Type the password again to verify it for **REPEAT PASSWORD**.
   - Click **CONFIGURE**.

   This is the account you will use to access the Turbonomic user interface with administrator permissions. *Be sure to save the user interface administrator account credentials in a safe place.*

   > **NOTE:**
   > The initial login is always for the `administrator` account. This is an administration *user* account. Do not confuse this with the Turbonomic System Administrator account that you previously set up to log into shell sessions on the VM itself.

10. After you have logged in as `administrator`, you can create other user accounts, and you can give them various roles. For more information about user accounts and roles, see the *Turbonomic User Guide*.

11. Optionally, synchronize the system clock.

    If you intend to use Single Sign-On (SSO) authentication, you need to synchronize the system clock.

    For information, see Synchronizing Time (Recommended) *(page 11)* and Single Sign-On Authentication *(page 14)*.

General Configuration Options

After you install Turbonomic, you should configure the machine's clock.

Synchronizing Time (Recommended)

It is important that you synchronize the clock on the Turbonomic instance with the devices on the same network. You will specify the servers that Turbonomic will use to synchronize its clock.

You should also set the system clock to your current time zone. Turbonomic runs regular data maintenance processes, and to minimize performance impact it runs these processes at night. To ensure that these processes run at the proper local time, you should synchronize the VM with your local time zone.

To synchronize the clock on the Turbonomic instance:

1. If it exists, back up your existing localtime config file.

   Execute the command: `sudo mv /etc/localtime /etc/localtime.bak`

2. Choose the zoneinfo file that matches your timezone.

   Select the file from the `/usr/share/zoneinfo` directory that matches your timezone. To see the files, execute the command: `sudo ls usr/share/zoneinfo`.

3. Link to the timezone file to your localtime directory.

   Create a symlink between your selected file (America/Chicago, in this example) and the localtime file. Execute the command:

   ```
   sudo ln -s -f /usr/share/zoneinfo/America/Chicago /etc/localtime
   ```

4. Verify that the new time settings have taken effect.

   Execute the `date` command. You should see results similar to:

   ```
   Thu Feb 2 14:25:45 CST 2018
   ```

To set up chrony on your Turbonomic instance:

1. Open an SSH terminal session to your Turbonomic instance.
2. Open the chrony configuration file.

   For example, execute the command: `sudo vi /etc/chrony.conf`
3. Replace the timeservers at the bottom of the file with your timeservers or use the default CentOS servers.
4. Save the file.
5. Restart the chrony service.

   Execute the command: `sudo systemctl restart chronyd`
6. Verify that your time is still correct.

   Execute the `date` command. You should see results similar to:

   ```
   Thu Feb 2 14:25:45 CST 2018
   ```

License Installation and First-time Login

Before you begin, make sure you have your full or trial license key file that was sent to you in a separate email. Save the license file on your local machine so you can upload it to your Turbonomic installation.

To use Turbonomic for the first time, perform the following steps:

1. Type the IP address of your installed Turbonomic instance in a Web browser to connect to it.
2. Log in to Turbonomic.
   - Use the default credential for **USERNAME**: `administrator`.
   - Type a password for **PASSWORD**.
   - Type the password again to verify it for **REPEAT PASSWORD**.
   - Click **CONFIGURE**.
3. Continue setting up your Turbonomic installation.

   Click **LET'S GO**.
4. Open the **Enter License** fly-out.

   Click **IMPORT LICENSE**.
5. Upload your license key file.
   a. In the Enter License fly-out, you can upload the license in one of the following ways:
      - Drag the license key file into the Enter License fly-out.
      - Browse to the license key file.

      Be sure to upload only .xml or .lic files.
   b. Click **SAVE**.

Depending on which license you have installed, the license enables either a trial or a full unlimited license for Turbonomic.

Single Sign-On Authentication

If your company policy supports Single Sign-On (SSO) authentication, Turbonomic enables SSO authentication by using Security Assertion Markup Language (SAML) 2.0.

At a high-level, the process involves:

- Creating external groups or at least one external user for SSO. See "Managing User Accounts" in the *Turbonomic User Guide*.
- Configuring Turbonomic to connect to the SAML Identity Provider (IdP). See Configuring Single Sign-On *(page 15)*.

When SSO is enabled, use your SSO credentials to log in to your Turbonomic instance. Do not use your local or Active Directory (AD) credentials for the login. The Identity Provider (IdP) will perform the authentication.

Prerequisites

Before you begin, make sure the IdP is set up for SSO. You can use a proprietary or public IdP. For examples of settings for a public Okta IdP, see What Are the Typical Settings for an IdP? *(page 26)*.

Configuring Single Sign-On

To configure Single Sign-On, perform these steps:

1. (Required) Create external groups or at least one external user for SSO.

   > **IMPORTANT:**
   > When SSO is enabled, Turbonomic only permits logins via the SSO IdP. Whenever you navigate to your Turbonomic installation, it redirects you to the SSO Identity Provider (IdP) for authentication before displaying the Turbonomic user interface.
   >
   > Before you enable SSO for your Turbonomic installation, *you must configure at least one SSO user with Turbonomic administrator privileges*. If you do not, then once you enable SSO you will not be able to configure any SSO users in Turbonomic. To authorize an SSO user as an administrator, use **EXTERNAL AUTHENTICATION** to do one of the following:
   >
   > - Configure a single SSO user with administrator authorization.
   >
   >   Add an external user. The username must match an account that is managed by the IdP.
   > - Configure an SSO user group with administrator authorization.
   >
   >   Add an external group. The group name must match a user group on the IdP, and that group must have at least one member.
   >
   > For information about creating external groups or external users for SSO, see "Managing User Accounts" in the *Turbonomic User Guide*.

2. Obtain a JSESSIONID cookie and make a record of it.

   To obtain a JSESSIONID cookie, use this curl command:

   ```
   curl -k -v 'https://<IP_Address>/vmturbo/rest/login' --data
   'username=administrator&password=<my_password>'
   ```

   where <IP_Address> is the IP address or host name of your Turbonomic instance and <my_password> is the password for your Turbonomic administrator user account.

   For example: `curl -k -v 'https://10.10.10.123/vmturbo/rest/login' --data 'username=administrator&password=welcome57!'`

3. (Required) Ensure that chrony is configured and the system time on your Turbonomic instance is correct.

   For instructions, see Synchronizing Time (Recommended) *(page 11)*.

4. Obtain the metadata from your IdP.

   a. Contact your security administrator to obtain the metadata from IdP.

   b. Save the metadata file in a directory on your local machine.

   c. Compare your metadata to the sample provided in Example of IdP Metadata *(page 17)*.

      If your metadata includes optional attribute tags that are not listed in the example, remove those optional attribute tags since they are not supported.

d. (Required) Name the metadata file: `metadata.xml`

5. Navigate to the local directory where you saved the metadata.xml file.
6. Upload the IdP metadata to import it.

   Run this curl command from the local directory where you saved the metadata.xml file:

   ```
   curl -v -k --cookie 'JSESSIONID=<jsessionid_value>' -X POST -F file=@metadata.xml
   https://<IP_Address>/vmturbo/rest/saml/idpmetadata
   ```

   where <jsessionid_value> is the JSESSION cookie that you previously obtained and <IP_Address> is the IP address or host name of your Turbonomic instance.

   For example: `curl -v -k --cookie 'JSESSIONID=node0p6lkwex749dcw5ipbne4rm970.node0' -X POST -F file=@metadata.xml https://10.10.10.123/vmturbo/rest/saml/idpmetadata`
7. Obtain a key store to support IdP.

   Generate a key store for SAML that supports IdP by using a security utility like Java SDK keytool.

   > **NOTE:**
   > During the process to generate a key store, you also create an alias. For the alias password, enter the same password that you used for the key store.

8. Save the key store file in the same local directory where you saved the metadata.xml file.
9. Obtain a certificate from IdP.

   Contact your security administrator to obtain a certificate from IdP.
10. Import the IdP certificate into the key store.
11. Install the key store.

    Run the curl command from the local directory where you saved the key store file:

    ```
    curl -v -k --cookie 'JSESSIONID=<jsessionid_value>' -X POST -F
    file=@<keystore_file_for_saml> https://<IP_Address>/vmturbo/rest/saml/keystore
    ```

    where <jsessionid_value> is the JSESSION cookie that you obtained, <keystore_file_for_saml> is your key store file for SAML, and <IP_Address> is the IP address or host name of your Turbonomic instance.

    For example: `curl -v -k --cookie 'JSESSIONID=node0p6lkwex749dcw5ipbne4rm970.node0' -X POST -F file=@samlKeystore.jks https://10.10.10.123/vmturbo/rest/saml/keystore`
12. Update the SAML configuration.

    Use curl to update the values for the SAML configuration:

    ```
    curl -k 'https://<IP_Address>/vmturbo/rest/saml' -H 'cookie:
    JSESSIONID=<jsessionid_value>' -H 'content-type: application/json' --data-binary
    '{"entityId":"<IdP_Audience_Restriction>","enabled":true,"externalIP":"<IP_Address>",
    "password":"<keystore_password>", "alias": "<priv_key_alias>"}'
    ```

    where <IP_Address> is the IP address or host name of your Turbonomic instance. For the `--data-binary` parameters, specify the following values:

    - entityId: The IdP's Audience Restriction property
    - enabled: Type `true` to enable SAML.

- externalIP: The host name or IP address of your Turbonomic instance
- password: The key store password
- alias: The alias for the private key

For example:

```
curl -k 'https://10.10.10.123/vmturbo/rest/saml' -H 'cookie:
JSESSIONID=node0p6lkwex749dcw5ipbne4rm970.node0' -H 'content-type: application/
json' --data-binary '{"entityId":"turbo","enabled":true,"externalIP":"10.10.10.123",
"password":"nalle123", "alias": "apollo"}'
```

13. Restart the API component.
    a. Open an SSH terminal session to your Turbonomic instance.
    b. Use sudo as root.
       ```
       sudo bash
       ```
    c. Restart your API component.
       ```
       turboctl restart api
       ```
14. Verify that the configuration is successful.
    a. Navigate to the Turbonomic User Interface.
       You will be automatically redirected to your IdP for authentication.
    b. Log in with the username that is a member of the external group or external user previously configured.
    c. Verify that the system time on your Turbonomic instance is correct.
       If the time is not synchronized, this might cause an `HTTP Status 401 -authentication failed` exception in the browser.
    d. If the configuration is not successful, look for an `HTTP Status 500` exception in the product log. If this exception exists, review your metadata for invalid optional attribute tags.

Example of IdP Metadata

This section provides an example of IdP metadata which may be useful when you are examining the optional attributes in your metadata.

If your metadata includes optional attribute tags that are not listed in the example, remove those optional attribute tags since they are not supported.

```
<?xml version="1.0" encoding="UTF-8"?>
     <md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
     entityID="http://www.okta.com/exkexl6xc9MhzqiC30h7">
     <md:IDPSSODescriptor WantAuthnRequestsSigned="false"
     protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
     <md:KeyDescriptor use="signing">
```

```
        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
        <ds:X509Certificate>
        MIIDpDCCAoygAwIBAgIGAWMnhv7cMA0GCSqGSIb3DQEBCwUAMIGSMQswCQYDVQQGEwJVUzETMBEG
        A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
        MBIGA1UECwwLU1NPUHJvdmlkZXIxEzARBgNVBAMMCmRldi03NzEyMDIxHDAaBgkqhkiG9w0BCQEW
        DWluZm9Ab2t0YS5jb20wHhcNMTgwNTAzMTk0MTI4WhcNMjgwNTAzMTk0MjI4WjCBkjELMAkGA1UE
        BhMCVVMxEzARBgNVBAgMCkNhbGlmb3JuaWExFjAUBgNVBAcMDVNhbiBGcmFuY2lzY28xDTALBgNV
        BAoMBE9rdGExFDASBgNVBAsMC1NTT1Byb3ZpZGVyMRMwEQYDVQQDDApkZXYtNzcxMjAyMRwwGgYJ
        KoZIhvcNAQkBFg1pbmZvQG9rdGEuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
        ugxQGqHAXpjVQZwsO9n8l8bFCoEevH3AZbz7568XuQm6MK6h7/O9wB4C5oUYddemt5t2Kc8GRhf3
        BDXX5MVZ8G9AUpG1MSqe1CLV2J96rMnwMIJsKeRXr01LYxv/J4kjnktpOC389wmcy2fE4RbPoJne
        P4u2b32c2/V7xsJ7UEjPPSD4i8l2QG6qsUkkx3AyNsjo89PekMfm+Iu/dFKXkdjwXZXPxaL0HrNW
        PTpzek8NS5M5rvF8yaD+eE1zS0I/HicHbPOVvLal0JZyN/f4bp0XJkxZJz6jF5DvBkwIs8/Lz5GK
        nn4XW9Cqjk3equSCJPo5o1Msj8vlLrJYVarqhwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQC26kYe
        LgqjIkF5rvxB2QzTgcd0LVzXOuiVVTZr8Sh57l4jJqbDoIgvaQQrxRSQzD/X+hcmhuwdp9s8zPHS
        JagtUJXiypwNtrzbf6M7ltrWB9sdNrqc99d1gOVRr0Kt5pLTaLe5kkq7dRaQoOIVIJhX9wgynaAK
        HF/SL3mHUytjXggs88AAQa8JH9hEpwG2srN8EsizX6xwQ/p92hM2oLvK5CSMwTx4VBuGod70EOwp
        6Ta1uRLQh6jCCOCWRuZbbz2T3/sOX+sibC4rLIlwfyTkcUopF/bTSdWwknoRskK4dBekFcvN9N+C
        p/qaHYcQd6i2vyor888DLHDPXhSKWhpG
        </ds:X509Certificate>
        </ds:X509Data>
        </ds:KeyInfo>
        </md:KeyDescriptor>
        <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:Nam
eIDFormat>
        <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:N
ameIDFormat>
        <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POS
T"
        Location="https://dev-771202.oktapreview.com/app/ibmdev771202_turbo2_1/exkex
l6xc9MhzqiC30h7/sso/saml"/>
        <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Red
irect"
        Location="https://dev-771202.oktapreview.com/app/ibmdev771202_turbo2_1/exkex
l6xc9MhzqiC30h7/sso/saml"/>
        </md:IDPSSODescriptor>
        </md:EntityDescriptor>
```

Disabling Single Sign-On

If for some reason you no longer want to use SSO, you can disable it for your Turbonomic installation. To disable Single Sign-On, perform these steps:

1. Update the SAML configuration to disable it.

   Use curl to update the values for the SAML configuration:

```
curl -k 'https://<IP_Address>/vmturbo/rest/saml' -H 'cookie:
JSESSIONID=<jsessionid_value>' -H 'content-type: application/json' --data-binary
'{"entityId":"<IdP_Audience_Restriction>","enabled":false,"externalIP":"<IP_Address>",
"password":"<keystore_password>", "alias": "<priv_key_alias>"}'
```

where <IP_Address> is the IP address or host name of your Turbonomic instance.

For the `--data-binary` parameters, specify the following values:

- entityId: The IdP's Audience Restriction property
- enabled: Type `false` to disable SAML.
- externalIP: The host name or IP address of your Turbonomic instance
- password: The key store password
- alias: The alias for the private key

For example:

```
curl -k 'https://10.10.10.123/vmturbo/rest/saml' -H 'cookie:
JSESSIONID=node0p6lkwex749dcw5ipbne4rm970.node0' -H 'content-type: application/json'
--data-binary '{"entityId":"turbo","enabled":false,"externalIP":"10.10.10.123",
"password":"nalle123", "alias": "apollo"}'
```

2. Restart the API component.
   a. Open an SSH terminal session to your Turbonomic instance.
   b. Use sudo as root.
      ```
      sudo bash
      ```
   c. Restart your API component.
      ```
      turboctl restart api
      ```
3. Verify that the configuration is successful.
   a. Navigate to the Turbonomic User Interface.

      You will no longer be redirected to your IdP for authentication. You will be redirected to the default Turbonomic login screen.
   b. Log in with a local account or an Active Directory (AD) account.

Support for Single Logout

If you are using the SSO feature, Turbonomic supports the Single Logout feature provided by Security Assertion Markup Language (SAML) 2.0. When you click **Logout** in the Turbonomic session that has SSO enabled, the SAML 2.0 Single Logout feature terminates the Turbonomic session, the browser session, the Identity Provider (IdP) session, and sessions at other Service Providers (SP) connected to the same IdP session.

If you want to use this feature, contact your security administrator to configure it.

The following are requirements:

- The `Single Logout` setting must be enabled on the IdP.
- The IdP needs to trust the Turbonomic SAML key store certificate.

If the IdP does not enable or support Single Logout, you need to manually log out from the IdP to fully log out from Turbonomic.

If you close the browser without clicking **Logout** or if your browser session times out, you can log in again provided the Turbonomic or the IdP session is valid.

Updating Turbonomic to a New Version

Turbonomic continually and rapidly innovates and improves all aspects of this product. This means that Turbonomic periodically releases newer versions of this product. You should check regularly to see if a new version is available.

When a new version is available, it is important to properly update your existing installed instance, rather than just install a new one. When you first installed Turbonomic, you put into place sophisticated data collection and analysis processes. Internal to the installation is an integrated database that retains performance data from across your virtual environment. Turbonomic uses this historical data for right-sizing, projecting trends, and other analysis. This means that the database is important to Turbonomic *and becomes more so over time*. Properly updating your installation of Turbonomic preserves the database for continued use.

Before you begin the update procedure:

- Make sure you have the email that Turbonomic sent to you with links to the Turbonomic `.0VA` file and to the ISO image.
- Ensure that the physical machine hosting the VM meets the minimum requirements (see Minimum Requirements *(page 5)*).

You can update your Turbonomic VM using the offline method or the online method if you have access to the Internet.

Offline Update

To perform an offline update of your Turbonomic installation:

1. Save a snapshot of your current Turbonomic VM.

   Before updating, you should properly shut down (not power off) the Turbonomic VM. To do so, type:

   ```
   sudo init 0
   ```

   Then, perform a snapshot (or clone the VM). This provides a reliable restore point you can turn to in the event that trouble occurs during the update. After you have the snapshot, bring the VM back online.

2. Download and attach the ISO image to the VM that runs Turbonomic.

Refer to the email you received from Turbonomic for links to the Turbonomic `.OVA` file and to the ISO image.

3. Mount the ISO image by logging in to vCenter.
   a. In vCenter, navigate to the Turbonomic VM.
   b. Right-click the VM and choose **Edit Settings**.
   c. In the CD/DVD Drive drop-down menu:
      i. Choose **Datastore ISO**.
      ii. Browse to the Turbonomic update ISO image and choose it.
   d. Ensure that the **Connect at power on** checkbox is selected.
4. Log in to the Turbonomic VM.

   Use SSH to log in to the Turbonomic VM using the turbo account and password.
5. Make the directory and mount the ISO image.

   Type:

   ```
   sudo su -
   mkdir /mnt/iso
   mount /dev/cdrom /mnt/iso
   ```
6. Verify the correct version of the ISO image is mounted.

   Type: `ls /mnt/iso`

   Verify that the ISO image contains the correct version for your update.
7. Load the latest Docker images.

   Type: `/mnt/iso/turboload.sh`
8. Execute these commands to update Turbonomic.

   ```
   exit
   /mnt/iso/turboupgrade.sh | tee /opt/turbonomic/t8c_upgrade_$(date +%Y-%m-%d_%H_%M_
   %S).log
   ```

   Wait until the script is finished. You should see the message:

   ```
   XL upgrade finished successfully
   ```
9. Clear your browser data and refresh your browser.

   After clearing the browser data and refreshing your browser, you have full access to Turbonomic features. However, features that rely on current analysis data will not be available until after a full market cycle — usually 10 minutes. For example, the Pending Actions charts will not show any actions until after a full market cycle.
10. Notify other users to clear their browser data and refresh their Turbonomic browser sessions.

Online Update

This method assumes that you have direct access to the Internet or access to the Internet through a proxy server.

To perform an online update of your Turbonomic installation:

1. Save a snapshot of your current Turbonomic VM.

   Before updating, you should properly shut down (not power off) the Turbonomic VM. To do so, type:

   ```
   sudo init 0
   ```

   Then, perform a snapshot (or clone the VM). This provides a reliable restore point you can turn to in the event that trouble occurs during the update. After you have the snapshot, bring the VM back online.

2. Open the charts_v1alpha1_xl_cr.yaml file.

   ```
   vi /opt/turbonomic/kubernetes/operator/deploy/crds/charts_v1alpha1_xl_cr.yaml
   ```

3. Edit the charts_v1alpha1_xl_cr.yaml file to specify Turbonomic version that you want to install.

   In the Global section, edit the value for the tag parameter. In this example, `7.17.4` has been changed to `7.17.5`.

   ```
   global:
   #  registry: index.docker.io
   #  imageUsername: turbouser
   #  imagePassword: turbopassword
     repository: turbonomic
     tag: 7.17.5
   ```

4. Save the file.

5. Start the online update.

   Execute the kubectl apply command:

   ```
   kubectl apply -f /opt/turbonomic/kubernetes/operator/deploy/crds/
   charts_v1alpha1_xl_cr.yaml
   ```

   This command will download the newer Docker images from the Docker Hub and then will upgrade the components.

   Wait until the update is finished. You should see the message:

   ```
   XL upgrade finished successfully
   ```

6. Clear your browser data and refresh your browser.

   After clearing the browser data and refreshing your browser, you have full access to Turbonomic features. However, features that rely on current analysis data will not be available until after a full market cycle — usually 10 minutes. For example, the Pending Actions charts will not show any actions until after a full market cycle.

7. Notify other users to clear their browser data and refresh their Turbonomic browser sessions.

Appendix A: Turbonomic Components

The following listings show the components that Turbonomic creates as part of the installation process.

Core Components For Turbonomic

- `rsyslog`
- `nginx`
- `consul`
- `auth`
- `clustermgr`
- `api`
- `market`
- `action-orchestrator`
- `topology-processor`
- `arangodb`
- `repository`
- `group`
- `history`
- `plan-orchestrator`
- `reporting`

Mediation Components For Turbonomic

- `mediation-actionscript`

- `mediation-appdynamics`
- `mediation-hpe3par`
- `mediation-hyperv`
- `mediation-netapp`
- `mediation-oneview`
- `mediation-pure`
- `mediation-ucs`
- `mediation-vcenter`
- `mediation-vcenterbrowsing`
- `mediation-vmax`
- `mediation-vmm`

Appendix B: What Are the Typical Settings for an IdP?

Before you begin configuring Single Sign-On (SSO), you need to make sure the IdP is set up for SSO.

Here are typical settings for a public Okta IdP which may be useful when you set up your IdP.

SAML Settings: GENERAL	
Setting	**Example**
Single Sign On URL	`https://10.10.10.123/vmturbo/saml/SSO`
Recipient URL	`https://10.10.10.123/vmturbo/saml/SSO`
Destination URL	`https://10.10.10.123/vmturbo/saml/SSO`
Audience Restriction	`urn:test:turbo:markharm`
Default Relay State	
Name ID Format	`Unspecified`
Application username	The username for the account that is managed by Okta
Response	`Signed`
Assertion Signature	`Signed`
Signature Algorithm	`RSA_SHA256`

SAML Settings: GENERAL	
Setting	**Example**
Digital Algorithm	SHA256
Assertion Encryption	Unencrypted
SAML Single Logout	Enabled
Single Logout URL	https://10.10.10.123/vmturbo/rest/logout
SP Issuer	turbo
Signature Certificate	Example.cer (CN=apollo)
authnContextClassRef	PasswordProtectedTransport
Honor Force Authentication	Yes
SAML Issuer ID	http://www.okta.com/$(org.externalKey)

SAML Settings: GROUP ATTRIBUTE STATEMENTS		
Name	**Name Format**	**Filter**
group	Unspecified	Matches regex:.*admin.*.