Datrium

Datrium DVX
Software Configuration

Version 5.2.1.0

VMware, Inc.

3401 Hillview Ave.

Palo Alto, CA 94304

www.vmware.com

Contents

DVX Software Configuration **1**

Requirements for DVX Software Configuration **3**

Pre-Day-Zero Host Check 3

ESXi Host Criteria for DVX Use (Minimum requirements) 5

DVX Software Configuration Prerequisites 6

1. Install the Data Node and Compute Node SSDs 7

2. Obtain a Computer for access to the Data Node 7

3. Determine Data Node Port Connections and IP Addresses 7

Teamed 25G Ports: D12x4B, D12x4C, D12x10D and F24x2B, F24x2D 8

Teamed 10G Ports: D12x4B 4x10G 10

10G Data Traffic: D12x4 10G 12

4. Provide DVX System Access to Datrium Support Servers 14

Configure Data Node and DVX (GUI) **16**

D12x4 Teamed Data Interface 16

Network Access for First-Time Connection to the Data Node 17

Requirements for zero configuration access to the Data Node 17

Ethernet Connection to the Data Node 18

Web Browser Access to the Data Node 19

Data Node Zero Configuration URL 19

Zero Configuration Connection Communication 20

Configure DVX Settings 20

DVX GUI Start Page 21

Data Node Network Configuration 21

Global Static Settings 22
Data Interfaces 22
Data Network Settings 24
Management Interfaces 24
Management Network Settings 25
Applying the Network Configuration 26
Changing Network Settings 27
vCenter Registration 28
Configure Data Node and DVX (CLI) 30
Network Access for First-Time Data Node Connection 30
Requirements for zero configuration access to the Data Node 30
Ethernet Connection to the Data Node 31
Zero-Configuration Access to the Data Node (SSH) 32
Data Node Zero Configuration URL 32
Using SSH to Connect to the Data Node 34
Serial Port Access for First-Time Connection to the Data Node 35
Data Node Login – Serial Port Connection 36
Using the CLI Setup Wizard 37
Separate Data and Management Traffic, Bonded Failover Data Interface 37
1. DVX System Access and Identification 38
2. Data Node Network Configuration 39
3. Register the Data Node with the vCenter Server 42
Verification and Additional DVX Configuration 45
Verify Gateway Access to the Support Server (DVX CLI) 45
Verify Floating IP Addresses 46

Additional Configuration – DVX GUI 46
Set Up Email Alerts 47
DVX GUI – Email Alerts 48
Configure Access to an NTP Time Server 48
DVX GUI – NTP Time Server Configuration 49
Configure Access to a Web Proxy and Save the Configuration 49
DVX GUI - Web Proxy Configuration 49
Additional Configuration – DVX CLI 50
Configure Access to a Web Proxy 50
Set Up Email Alerts 50
Configure Access to an NTP Time Server 52
Terminate the CLI Session 52
Enable Blanket Encryption 53
User management 54
Configure Active Directory 54
Disable Active Directory Configuration 55
Show Active Directory Configuration Settings 55
Configure RBAC for DVX 56
Remove an AD Group from the DVX System 56
Show RBAC Settings 57
Upload a custom certificate 57
Verify the Certificates 58
2. Unregister vCenters from your DVX system 59
3. Upload a custom certificate 60
4. Clear old certificate from browser 62

5. Re-register vCenters with the DVX System 63
Optional: Regenerate a self-signed certificate 63
DVX Network Support 64
Data and Management Subnets 65
Data Node Network Ports 65
2x25G Data Node Ports: D12x4B, D12x4C, D12x10D and F24x2B, F24x2D 65
4x10G Data Node Ports: D12x4C 67
Network Traffic Payload Size (Jumbo Frames) 69
Data Node High Availability 69
Controller Redundancy 70
Floating IP Address 71
Network Port Redundancy 71
DVX Network Interface Pairs for Data and Management Traffic 72
Data Node Fault Tolerance (DNFT) 73
DNFT and “Reserved” Storage 74
Network Topology 74
Active Data Paths 74
Redundant Topology 76
DVX Network – High Availability 77
Network Topology – Teamed Data Ports 78
Network Support for Replication 79
Open Source & Third party software license notices 81
Source Code Offer 81
Data Node (Datrium OS) 81
Additional License Notices 98

Intel License 98
platform.py 99
ptmalloc3 99
Original SSLeay License 100
vprintf License 101
DVX Hyperdriver 102
KVM Hyperdriver 104
Cloud DVX 104
ControlShift Backend 104
Datrium GUIs 106
DVX GUI 106
ControlShift GUI 109
Additional License Notices 111

DVX Software Configuration

When you configure the DVX System you perform the following tasks:

- Pre-Day-Zero Host Check – Verify Compute Node suitability for DVX use, before installing the Data Node.
- **Data Node configuration**:
  - Configure DVX System settings (admin account password and DVX name).
  - Configure Data Node network interfaces.
  - Register your vCenter Server on the Data Node.
  - Configure additional DVX System settings (alert recipients, NTP server, and web proxy).
- **Add hosts to the DVX System**:
  - Configure the DVX System. (If you did not do this during Data Node configuration, do it now.)
  - Install the DVX Hyperdriver on the host(s).
  - Configure SSDs for DVX use. This process automatically mounts the Datrium datastore.

You can use the DVX GUI or the CLI setup wizard to configure the DVX System.

1. Before you start, read DVX Software Configuration Prerequisites .
2. To use the DVX GUI to configure the Data Node:

   - First-time browser access to the Data Node:
     Network Access for First-Time Connection to the Data Node
   - To continue with Data Node configuration:
     Configure DVX Settings
     Data Node Network Configuration
     vCenter Registration

   To use the DVX CLI to configure the Data Node:

- First-time access:
  Network Access for First-Time Data Node Connection

  > **Important:** After you finish Data Node configuration over the serial port, unplug the serial port cable from the Data Node. Do not leave the serial port cable connected to the Data Node when it is disconnected at the other end as this will produce electrical noise on the Data Node serial port. (CLI)

- To continue with Data Node configuration: Using the CLI Setup Wizard

3. To verify the network configuration, use the CLI:

- Verification and Additional DVX Configuration

2. To add hosts to the DVX System, use the DVX GUI Web Client Plug-in. For information, see “Host Configuration for DVX System Use” in the *DVX System Management* manual.

For information about the DVX System network environment, see DVX Network Support.

Requirements for DVX Software Configuration

The DVX Data Node as delivered contains all of the DVX software.

DVX Software Component	Description
DVX Data Node software	The Data Node software is the DVX file system software that runs on the Data Node. Data Node software is pre-installed.
DVX Hyperdriver software	The Hyperdriver is DVX file system software that runs on each host that will use Datrium storage. The Hyperdriver software is distributed in a VIB (VMware Installation Bundle).
DVX VAAI software	The VAAI support software runs on each host. It is contained in a separate VIB.
DVX GUI	The DVX GUI is a standalone GUI that runs on the Data Node.
DVX Web Client GUI	The DVX Web Client GUI is a vSphere Web Client plug-in.

Pre-Day-Zero Host Check

Prior to receiving a DVX System from Datrium, you can use Datrium software to check host suitability for DVX use.

1. Login to your Datrium Support account.
2. Download the datrium-hyperdriver-esx VIB.
3. Install the datrium-hyperdriver-esx VIB on any host that you will use with the DVX System.

   Before you add the host to the DVX System, you can use Datrium software to check host suitability for DVX use. Log in to the host and use the following command to install the datrium-hyperdriver-esx VIB.

   ```
   esxcli software vib install -v file://
   [host/]path/datrium-hyperdriver-esx_2.0.1.0-24008.zip
   ```

The host portion of the command is optional. If you copy the Hyperdriver zip file to the host, it is not needed. If you put the zip file in a location to be accessed over the network, specify the host.

You can also upload the Hyperdriver VIB to VUM and use VUM to manage the installation.

The datrium-hyperdriver-esx VIB provides a Datrium extension to both the `esxcli` and `localcli` commands. After installing the Hyperdriver VIB, you must reboot the host to use the esxcli Datrium extension.

> **Note:** After installing the hyperdriver VIB on the ESXi host, sometimes the Datrium namespace is not added to the esxcli command. In this case, you will see the following error:
>
> ```
> esxcli datrium
> Error: Unknown command or namespace datrium
> ```
>
> This can be fixed by restarting hostd on the ESXi host. To restart hostd, SSH into the host as root, and then run this command:
>
> ```
> /etc/init.d/hostd restart
> ```
>
> Alternatively, you can run the `localcli` command to access the datrium namespace without the need to restart the hostd. For example:
>
> ```
> localcli datrium
> ```

You can use `localcli` Datrium extension before rebooting. The picture below shows an example of `esxcli datrium check` output.

```
>> esxcli datrium check
Test                            Value                                                Result
------------------------------  ---------------------------------------------------  ------
CPU                             24 cores                                             OK
Memory                          255.87 GiB                                           OK
NIC speed                       10 Gbps or faster                                    OK
ESXi version                    6.0.0 (3620759)                                      OK
ESXi boot type                  visor-thin                                           OK
Lockdown mode                   Not enabled                                          OK
RAM disk                        Can create 1000 MiB RAM disk                         OK
Root partition                  32512 KiB free                                       OK
Scratch location                /vmfs/volumes/573f4787-5ca51e2b-1478-5cb9019ad89c     OK
Persistent logging              Yes                                                  OK
vSphere Flash Read Cache (vFRC) Not enabled                                          OK
Content-Based Read Cache (CBRC) Not enabled                                          OK
vSAN                            Not enabled                                          OK
Incompatible VIBs               Not found                                            OK
RAID controller CLI             HP hpssacli installed                                OK
Incompatible storage drivers    Not found                                            OK
```

The check command indicates the results of various tests. For optimal DVX System operation, all results should be “OK”. You should resolve any situations indicated by any other result. The following table shows the minimum requirements for DVX use.

ESXi Host Criteria for DVX Use (Minimum requirements)

Host Criteria	Minimum Requirement
CPU	8 CPU cores in total
Memory	10 GiB RAM
NIC speed	one vSwitch with at least one 10+ Gbps NIC
ESXi version	ESXi 5.5 Update 2 or later
ESXi boot type	installable or embedded
Lockdown mode	Not enabled
RAM disk	Host has enough memory to for 1600 MiB RAM disk space
Root partition	10 MiB free space
Scratch location	Scratch location is configured and writable
Persistent logging	Host has configured persistent vmkernel logging

Host Criteria	Minimum Requirement
Encryption AES-NI	CPU supports AES-NI (Advanced Encryption Standard New Instructions); AES-NI should be enabled
vSphere Flash Read Cache (vFRC)	Not in use
Content-Based Read Cache (CBRC)	Not enabled
vSAN	Not enabled
Incompatible VIBs	No incompatible third-party VIBs such as the one from PernixData
RAID Controller CLI	For host with MegaRaid, Dell or HP RAID controllers, the vendor-specific CLI utility should be installed: • MegaRaid: storcli • Dell: perccli • HP: hpssacli
Incompatible storage drivers	No incompatible storage drivers running, e.g. the lsi_mr3 driver on ESXi 5.5

DVX Software Configuration Prerequisites

You must satisfy the following prerequisites before you start the software configuration.

1. Install the Data Node and Compute Node SSDs
2. Obtain a Computer for access to the Data Node
3. Determine Data Node Port Connections and IP Addresses
4. Provide DVX System Access to Datrium Support Servers

1. Install the Data Node and Compute Node SSDs

Install the Data Node in a rack, connect it to the rack power sources, and connect it to your network. Make sure that you have installed Compute Node SSDs for DVX use. For more information, see the *Datrium DVX Hardware Installation* manual.

2. Obtain a Computer for access to the Data Node

Obtain a computer that you can use for DVX software configuration. You can perform the software configuration with or without network access to the Data Node.

- **Zero configuration access**– If you have multicast DNS responder software on your system, you can use an ethernet cable to create a direct connection to the Data Node. For information about zero configuration access, see Configure Data Node and DVX (GUI).
- **Serial port access** – If you do not use zero configuration access, you must use a serial port connection to the Data Node. Your computer must be capable of supporting the serial port connection. Datrium supplies a serial port cable in the Data Node shipping package. The serial cable provides a standard DB9 connector.

Use the following serial port settings:

Serial port speed	115200	Stop bit	1
Data bits	8	Parity	None

3. Determine Data Node Port Connections and IP Addresses

The DVX System supports both data and management traffic. The data interfaces support Adaptive Pathing networking for aggregate network bandwidth. The management interfaces can support bonded pair operation as an active/passive redundant interface.

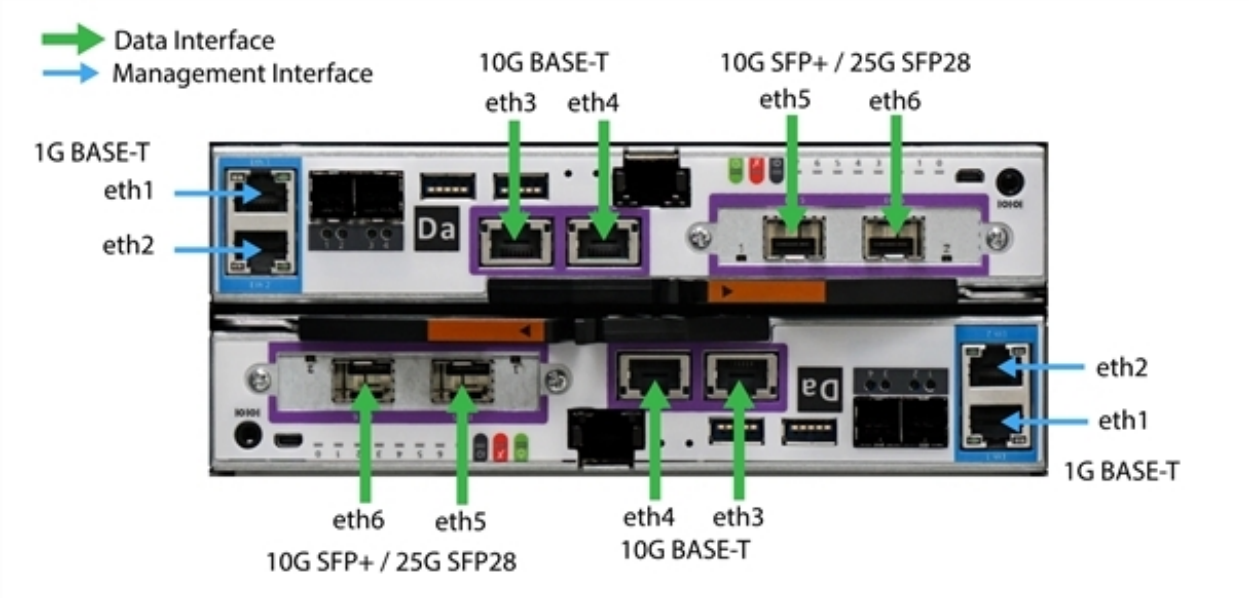
Use the Data Node network interfaces that correspond to the ports that you have connected to your network. (See *Datrium DVX Hardware Installation*.) For information about DVX network configuration, see DVX Network Support.

The options that you have for network configuration are determined by the type of DVX Data Node that you are using. DVX Data Nodes support 10 BASE-T, SFP+, or SFP28 media types for data traffic, depending on the Data Node model. All Data Nodes support 1G BASE-T for management traffic.

- Teamed 25G Ports: D12x4B, D12x4C, D12x10D and F24x2B, F24x2D
- Teamed 10G Ports: D12x4B 4x10G
- 10G Data Traffic: D12x4 10G

Teamed 25G Ports: D12x4B, D12x4C, D12x10D and F24x2B, F24x2D

The D12x4B, D12x4C, D12x10D, F24x2B, F24x2D models provide 1G BASE-T management interfaces, and 10G BASE-T and 10GSFP+/25G SFP28 data interfaces.



- For data traffic, use one of the following 10G port teams. You cannot mix different port types in a team.

  eth3+eth4 OR eth5+eth6

- For management traffic, use a single management interface (eth1 OR eth2).

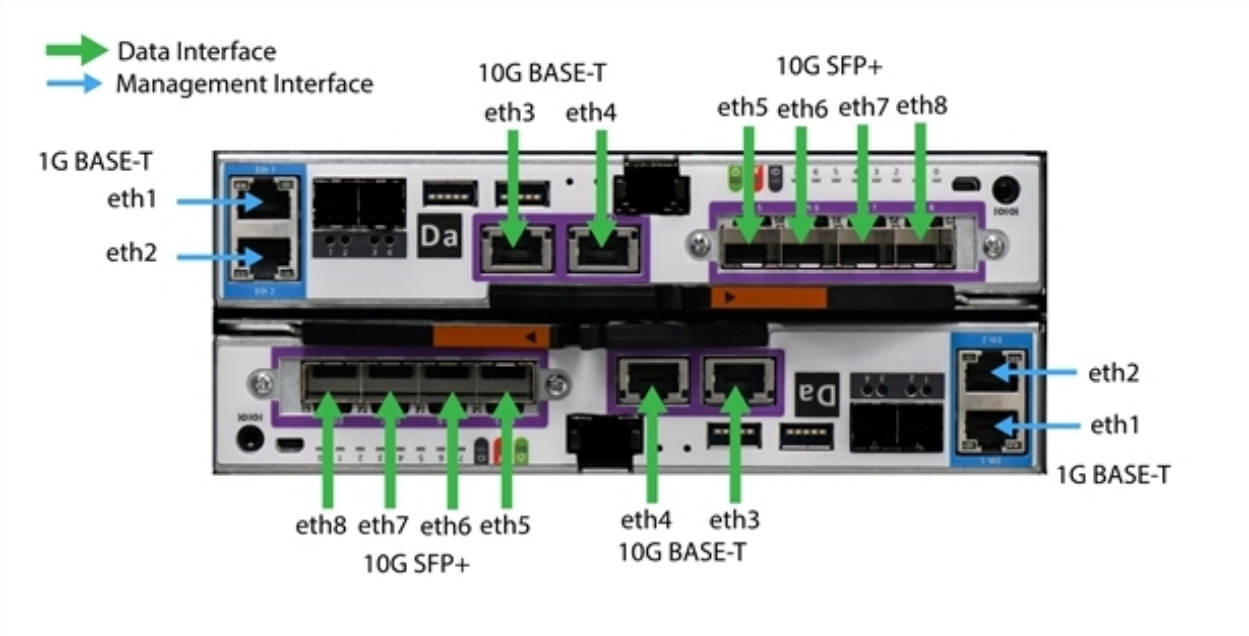
You must supply the following IP addresses:

- 5 IP addresses for the data interface – two for the data ports on each controller, plus a data floating IP address.
- 3 IP addresses for the management interface – one for the management port on each controller, plus a management floating IP address.
- A gateway IP address for access to the Internet.
- If you are using an HTTP proxy for access to the Internet, you must configure the proxy address on the Data Node for access to Datrium Support.
- If you are using one or more DNS servers, you must configure them on the Data Node.

IP Addresses for Separate Data and Management Traffic		
DVX System Usage	**Address**	**Interfaces (for the connected ports)**
Controller1 data ports	IP: IP:	
Controller2 data ports	IP: IP:	
Data Floating IP address	IP:	n/a
Controller1 management port	IP:	
Controller2 management port	IP:	
Management Floating IP address	IP:	n/a
Gateway IP address	IP:	n/a
HTTP proxy IP address (if necessary)	IP:	n/a
DNS server IP address(es) (if necessary)	IP:	n/a

Teamed 10G Ports: D12x4B 4x10G

The D12x4B 4x10G model provides 1G Base-T management interfaces and 10G BASE-T and SFP+ interfaces data interfaces.



- For data traffic, use one of the following 10G port teams. You cannot mix different port types in a team.

  eth3+eth4 OR eth5+eth6 OR eth7+eth8 OR eth5+eth6+eth7+eth8

- For management traffic, use a single management interface (eth1 OR eth2).

You must supply the following IP addresses:

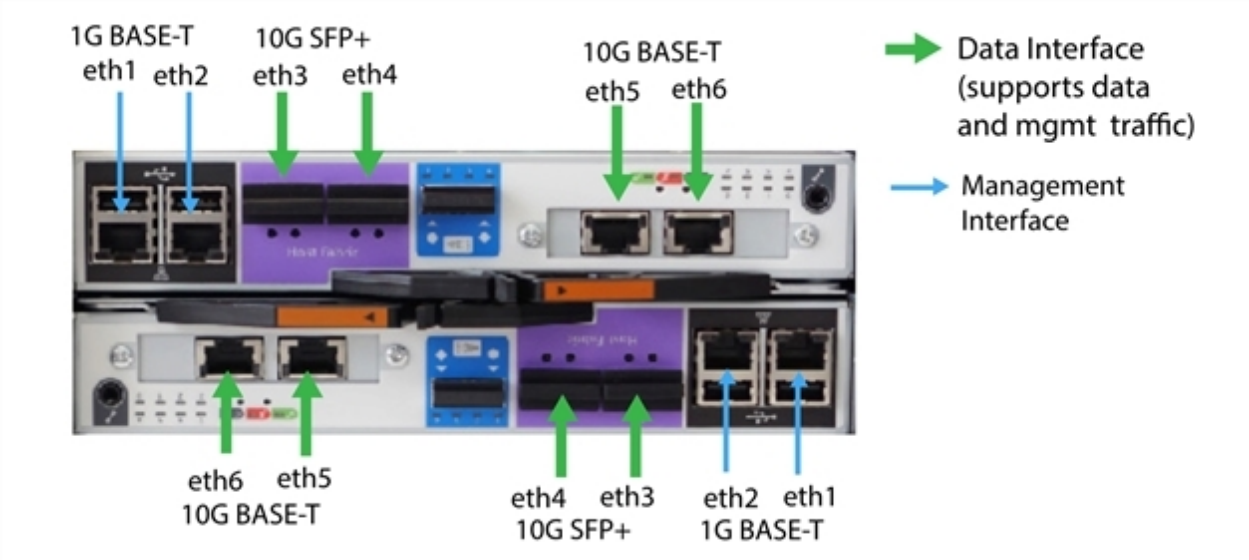
- 5 or 9 IP addresses for the data interface – two or four for the data ports on each controller, plus a data floating IP address.
- 3 IP addresses for the management interface – one for the management port on each controller, plus a management floating IP address.
- A gateway IP address for access to the Internet.
- If you are using an HTTP proxy for access to the Internet, you must configure the proxy address on the Data Node for access to Datrium Support.

- If you are using one or more DNS servers, you must configure them on the Data Node.

IP Addresses for Separate Data and Management Traffic		
DVX System Usage	**Address**	**Interfaces (for the connected ports)**
Controller1 data ports	IP: IP: IP: IP:	
Controller2 data ports	IP: IP: IP: IP:	
Data Floating IP address	IP:	n/a
Controller1 management port	IP:	
Controller2 management port	IP:	
Management Floating IP address	IP:	n/a
Gateway IP address	IP:	n/a
HTTP proxy IP address (if necessary)	IP:	n/a
DNS server IP address(es) (if necessary)	IP:	n/a

10G Data Traffic: D12x4 10G

The D12x4 Data Node provides a choice of 10G SFP+ or 10G BASE-T data interfaces, along with the 1G BASE-T management interfaces.



The example configuration supports two 10G teamed ports for adaptive path data traffic and a single separate 1G network interface for management traffic. Use the interfaces that correspond to the ports that you connected to your network.

- For data traffic, use one of the following 10G port pairs. You cannot mix different port types in a teamed pair.

  eth3+eth4 OR eth5+eth6

- For management traffic, use a single management interface (eth1 OR eth2).

You must supply the following IP addresses:

- 5 IP addresses for the data interface – two for the data ports on each controller, plus a data floating IP address.
- 3 IP addresses for the management interface – one for the management port on each controller, plus a management floating IP address.
- A gateway IP address for access to the Internet.

- If you are using an HTTP proxy for access to the Internet, you must configure the proxy address on the Data Node for access to Datrium Support.
- If you are using one or more DNS servers, you must configure them on the Data Node.

IP Addresses for Separate Data and Management Traffic		
DVX System Usage	**Address**	**Interfaces (for the connected ports)**
Controller1 data ports	IP: IP:	
Controller2 data ports	IP: IP:	
Data Floating IP address	IP:	
Controller1 management port	IP:	
Controller2 management port	IP:	
Management Floating IP address	IP:	
Gateway IP address	IP:	n/a
HTTP proxy IP address (if necessary)	IP:	n/a
DNS server IP address(es) (if necessary)	IP:	n/a

4. Provide DVX System Access to Datrium Support Servers

When you configure the network interface(s) on the Data Node, you provide the IP address for a gateway to the Internet. This is necessary to support DVX System access to the Datrium Auto Support, Remote Support, and Upgrade servers. This table shows the network interface information for this access.

DVX Capability	Subnet	Data Node Interface	Datrium Server, Port, and Protocol
Auto Support	Management subnet	Management interface: Floating IP address and both controller IP addresses	server: autosupport.datrium.com port: 443 protocol: HTTPS
Remote Support	Management subnet	Management interface: Floating IP address and both controller IP addresses	servers: autosupport-tunnel.datrium.com autosupport-tunnel-https.datrium.com port(s): 443 (autosupport-tunnel) 443 (autosupport-tunnel-https) protocol: HTTPS
Software Upgrade	Management subnet	Management interface: Floating IP address and both controller IP addresses	server: upgrade-center-01.datrium.com port: 443 protocol: HTTPS

The table below shows DVX System port usage.

DVX Usage	Ports
Data Node	80, 443, 2181, 4075, 4085, 4099, 7443, 9081, 9443

DVX Usage	Ports
Hyperdriver	1044, 1522, 1525, 1608, 1901, 2020
Zero configuration client system	5353 (UDP)
Firewall access for replication	4105 (Data Node to Data Node) 1525 (DVX host(s) to DVX host(s))
Firewall access for Datrium Support	443 (see DVX Software Configuration Prerequisites)
Cloud DVX	4105 and 1758 (Data Pool to/from Cloud) 443 (outbound traffic to AWS services)
DVX SDK	443
Datrium SRA	443

Configure Data Node and DVX (GUI)

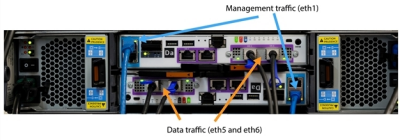
The DVX System provides a Data Node GUI that you can use to perform Data Node and DVX configuration. Before you start the software configuration, make sure you have satisfied the Requirements for DVX Software Configuration. The Data Node ports that you intend to use should be connected to your network. The same ports on both controllers must be connected to the network.

The GUI examples are based on the following configuration:

- Static IP address configuration.
- Separate data and management subnets.
- Adaptive path teamed network port configuration for the Data Node data interfaces.

D12x4 Teamed Data Interface

The picture below shows an example of cable connections for a similar configuration. The figure shows the use of an SFP+ port pair (eth3/eth4 - black cables) for data traffic and the 1Gb BASE-T interface (eth1) for management traffic (orange cables). The example in this manual uses the 10base-t port pair (eth5/eth6) for data traffic.



For information about the DVX network environment, see DVX Network Support.

The following sections describe how to use the DVX Data Node GUI to configure the Data Node.

- Network Access for First-Time Data Node Connection
- Configure DVX Settings
- Data Node Network Configuration
- vCenter Registration

After you have completed vCenter Server registration, you can perform Verification and Additional DVX Configuration and then log in to the vSphere Web Client and use the DVX GUI to add Compute Nodes to the DVX System. For information about adding hosts to the DVX System, see the *DVX System Management* manual.

Network Access for First-Time Connection to the Data Node

The DVX System supports a zero configuration (zeroconf) connection to the Data Node. The Data Node provides a zeroconf service that uses the Avahi implementation of the zeroconf specification. The Data Node uses the mDNS multicast protocol to support the zeroconf connection.

Requirements for zero configuration access to the Data Node

The system that you use to connect to the Data Node must have the multicast DNS responder daemon and your system must allow access over UDP port 5353.

Multicast DNS responder software is available on different operating system platforms as part of various software packages.

Windows	You must install responder daemon software. Examples of software that is available for Windows and includes the multicast DNS responder are iTunes and the Apple Bonjour Print Services.
OS X	The responder daemon software is part of Mac Os X.
Linux	You must install the Avahi and nss-mdns packages that are appropriate for your particular Linux distribution. The following nss-mdns links might be useful: http://0pointer.de/lennart/projects/nss-mdns/ https://launchpad.net/ubuntu/+source/nss-mdns http://rpmfind.net/linux/rpm2html/search.php?query=nss-mdns

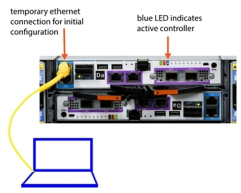
	It might be necessary to start the Avahi daemon. If your browser cannot resolve the Data Node Zero Configuration URL, use the avahi-autoipd command to acquire a link local address. `avahi-autoipd -D network-interface [--force-bind]` Use the --force-bind argument only if you cannot bind a link local address to a dedicated interface that is not configured with a routable IP address.

The Data Node uses an IPv4 link-local IP address in the address block 169.254.0.0/16. The operating system on your client system must be able to use the link-local subnet to respond to the Data Node.

Ethernet Connection to the Data Node

For initial configuration, use an Ethernet cable to connect your laptop or other client system directly to the eth1 management port on the Data Node. Make sure to connect to the management port on the active controller. The temporary connection provides access for the CLI session.

The figure below shows a Data Node that does not have any other network connections. It is not necessary to connect the Data Node to your network to perform initial configuration, but you can do so if desired.



When you save the network configuration, the DVX System will disable the zeroconf connection. At that time, replace the temporary connection with a connection between the configured management port and the management subnet. Then you can use the management floating IP address to log in over the management subnet. If you have not already connected the other ports that you have configured, do so at this time.

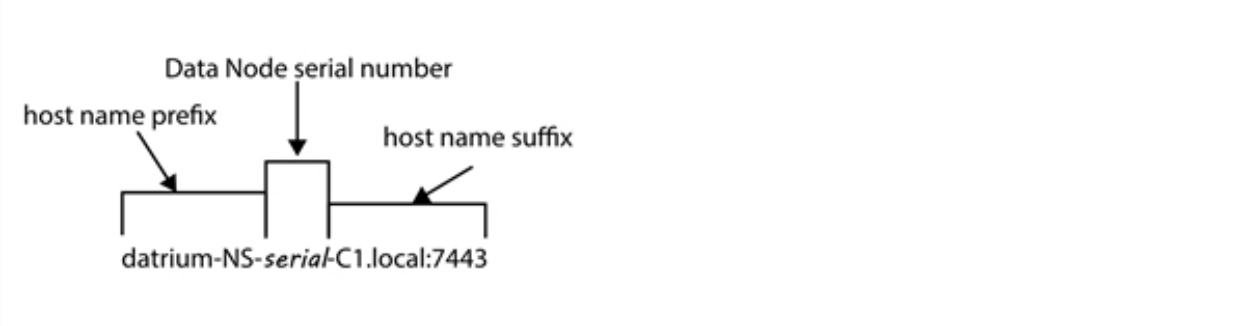
Web Browser Access to the Data Node

To connect to the Data Node, specify the Data Node zeroconf URL in your browser window.

Data Node Zero Configuration URL

The Data Node zeroconf URL contains the Data Node host name. The host name has three components:

- Host name prefix – "`datrium-NS-`".
- Data Node serial number – The serial number is on the back of the chassis (see below).
- Host name suffix – Identifies the active controller on the Data Node.



Controller	Host name suffix
1	`-C1.local:7443`
2	`-C2.local:7443`

The Data Node serial number is located on the inside of the left "ear" of the PCM on the left side of the Data Node.

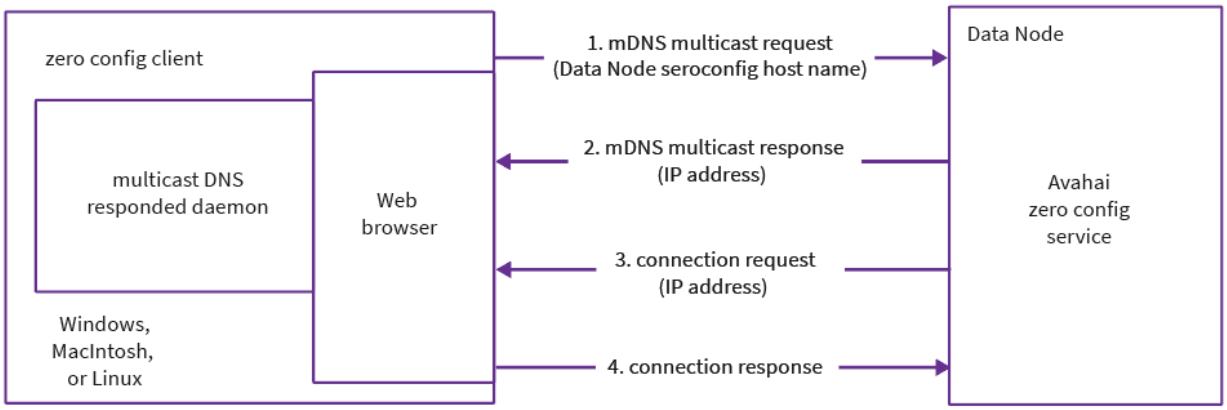
The following string is an example of a zeroconf URL with a Data Node serial number of 000000000000000:

```
https://datrium-NS-000000000000000-C1.local:7443
```

It may take a few minutes to establish the zeroconf connection. Ping the Data Node zeroconf URL to determine connectivity.

Zero Configuration Connection Communication

1. When you enter the Data Node zeroconf URL in the browser, your system sends an mDNS multicast message to obtain an IP address for the Data Node host name.
2. The Data Node responds to the multicast message and sends back its IP address.
3. The browser uses the Data Node IP address to establish a connection.
4. The Data Node responds to the connection request to begin the session.

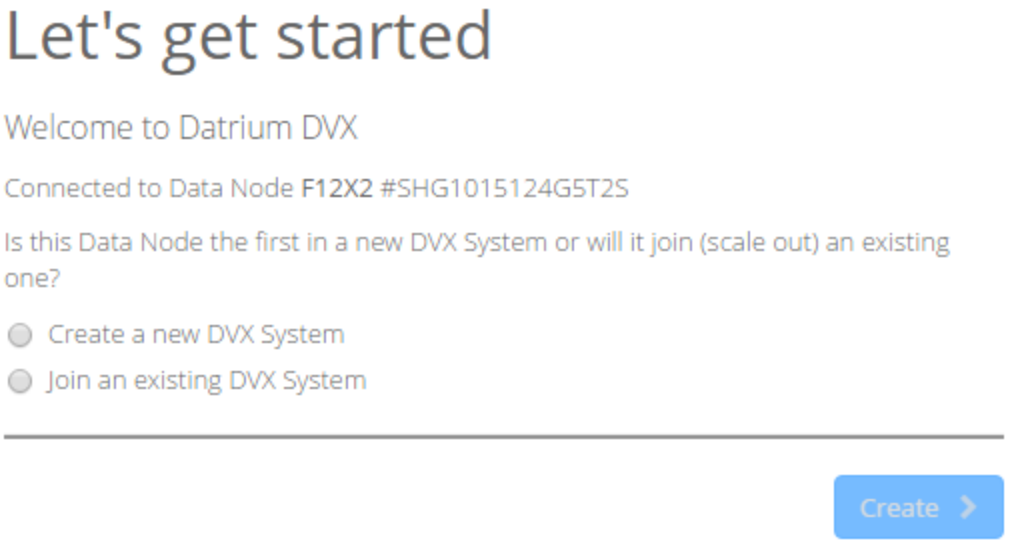


When you connect to the Data Node for the first time, use the default password “datrium#1” to log in to the system.

Configure DVX Settings

After you log in, the GUI displays the start page. This page gives you the option of creating a new DVX System or joining an existing System. For information about adding a Data Node to an existing DVX System, see “Expanding the Data Pool” in the DVX System Management manual.

DVX GUI Start Page



Select the ”Create a new DVX System” toggle and click the “Create >” button to start the configuration process. You must log in again, then the GUI displays the DVX Settings page. Use the DVX settings page to specify the DVX name and admin account password.

- The DVX GUI displays the DVX name on the dashboard and it uses it as the prefix for the Datrium datastore name.
- The admin account on a new Data Node has the default password `datrium#1`. To keep the current password, leave the password fields blank; however, we recommend that you create a new password that contains at least 10 characters, including a combination of uppercase and lowercase letters, numbers, and special characters.

Data Node Network Configuration

When you perform network configuration, you specify global IP settings, Data Node interfaces, and IP addresses and netmasks.

> **Important:** When you press the Configure network button at the bottom of the page, the DVX System applies the new network configuration and then terminates the zeroconf connection. If the DVX System applies the configuration successfully, it

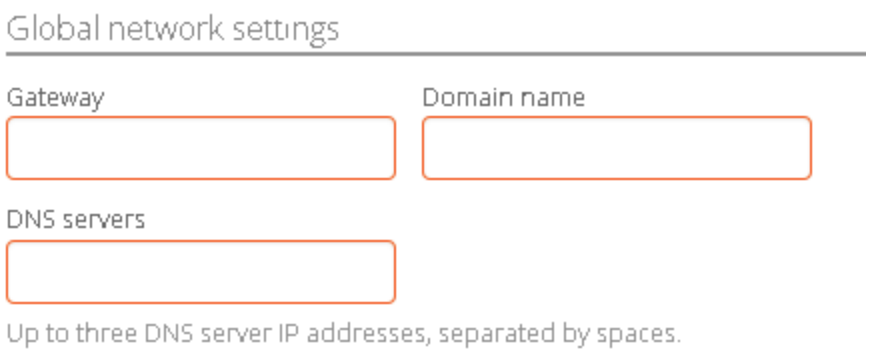
displays the Network changed page. This page contains a link for the management floating IP address and the Continue button.

To commit the network configuration, use the link the Continue button to log in to the Data Node. You have 10 minutes after you click Configure network to log in again. If you do not log in within the 10-minute time period, the DVX System will roll back the network settings. See Applying the Network Configuration.

The following sections describe the input fields for Data Node network configuration

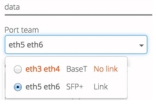
Global Static Settings

You must configure a gateway to the Internet so that the DVX System has access to the Datrium Support server at autosupport.datrium.com. The gateway must be on the same subnet as the Data Node interface that you are using for management traffic. You must also set the domain name for the Data Node. You can also define access to a maximum of three DNS servers.



Data Interfaces

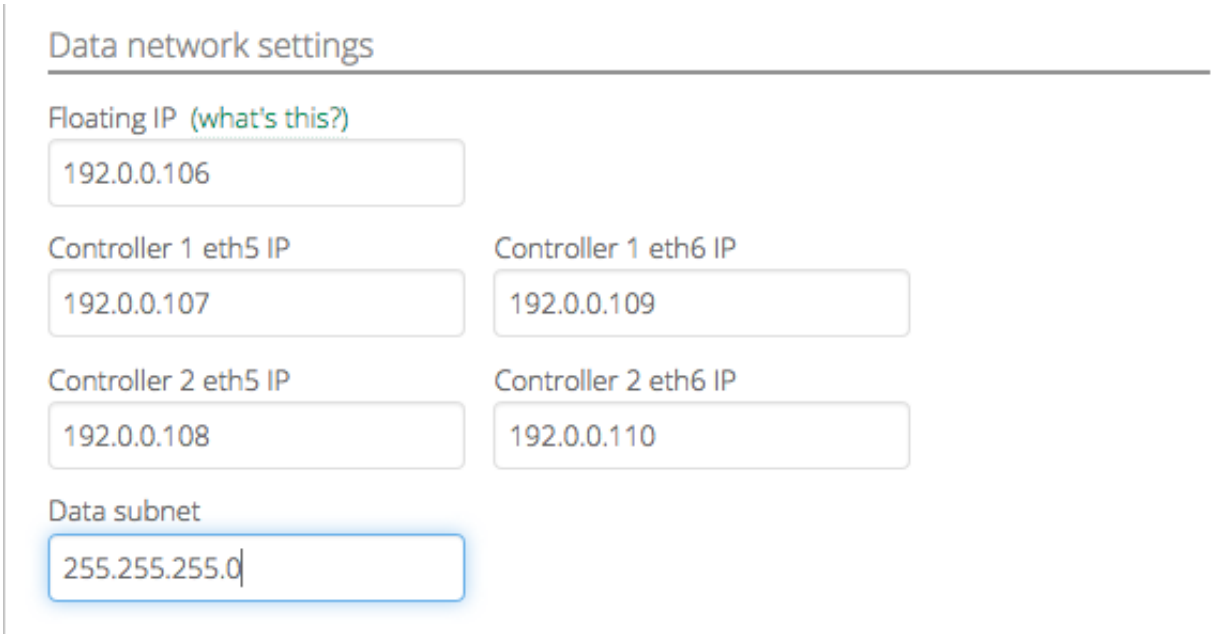
Identify the Data Node network ports that you will use for data traffic. You have the choice of teamed network interfaces for data traffic using either 10GBaseT or SFP media. The DVX System will use the ports of the teamed interface for aggregate data traffic. If there is a network failure on one of the ports, the System will continue to use the remaining active port for data traffic. Select one of the following interface specifications for the data path:

Interface Specification	Data Node Models	Interface Type
eth3+eth4	D12x4 D12x4B 4x10G D12x4C 2x25G D12x10D 2x25G F24x2B 2x25G F24x2D 2x25G	10Gb BASE-T RJ45 Ethernet
eth5+eth6	D12x4B 2x25G D12x10D 2x25G F24x2B 2x25G F24x2D 2x25G	10Gb SFP+ / 25Gb SFP28 (direct attach twin axial copper or optical)
eth5+eth6	D12x4 D12x4B 4x10G	10Gb SFP+ (direct attach twin axial copper or optical)
eth5+eth6+eth7+eth8	D12x4B 4x10G	10Gb SFP+ (direct attach twin axial copper or optical)
An interface specification represents the same port(s) on both controllers on the Data Node. When you apply the network configuration, the DVX System configures the same port(s) on both controllers to support controller failover. The GUI indicates the interfaces that are connected to the network. In this example, the ports for the eth5 and eth6 interface are connected.		

Data Network Settings

This example requires five IP addresses and a netmask for the teamed data interface.

- You must supply a floating IP address for data traffic. The Hyperdriver on a host uses the data floating IP address to communicate with the Data Pool. The DVX System uses the floating IP address to support the High Availability capability in the event of controller failover. Regardless of any controller failover that might occur in a Data Pool, the DVX System maintains the floating IP address for continued access.
- You must supply IP addresses for both controllers.
- The subnet mask is the dot-decimal representation of the network mask for the data interface.



Management Interfaces

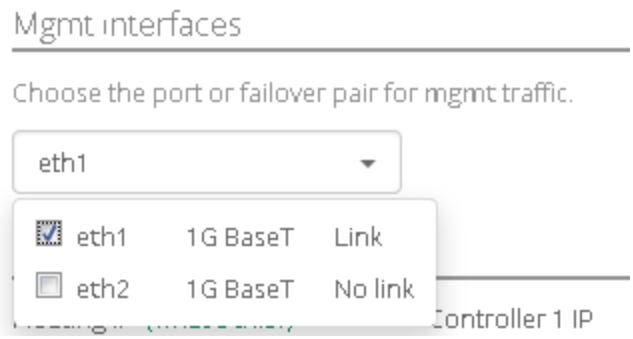
Identify the Data Node network ports that you will use for management traffic.

- An interface specification represents the same port(s) on both controllers on the Data Node. When you execute the command, the DVX System configures the same ports on both controllers to support controller failover.

- You can specify a single interface or, to support management network failover, you can specify both 1Gb interfaces.
- Use one of the following interface specifications for the management path:

  eth1
  eth2
  eth1 eth2

The example below shows the selection of the eth1 interface.



Note that some of the management connections that originate from the DVX Data Node use the physical management IP address of the interface.

Management traffic, in addition to using the management floating IP address, requires the use of the physical management IP addresses on both controllers (eth1 or eth2, or both eth1 and eth2 for bonded management interfaces).

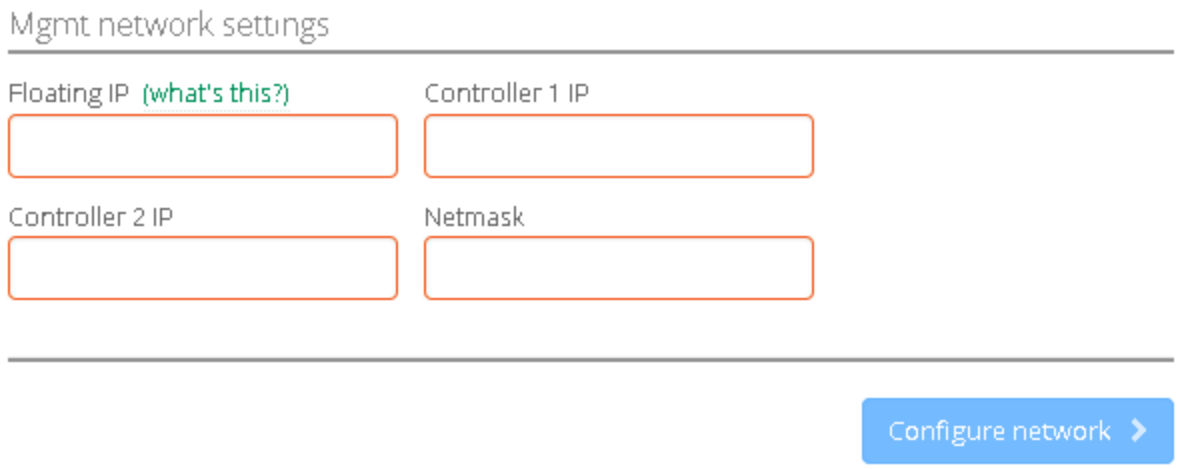
Management Network Settings

You must provide three IP addresses and a netmask for the selected management interface (s).

- You must supply a floating IP address for management traffic. The DVX GUI uses the management floating IP address to communicate with the Data Pool. The management floating IP address also supports DVX CLI and DVX GUI connections to the DVX System. The DVX System uses the floating IP address to support the High Availability capability in the event of controller failover. Regardless of any controller failover that might occur in a Data Pool, the DVX System maintains the floating IP address for continued access.

- You must supply IP addresses for both controllers.
- The subnet mask is the dot-decimal representation of the network mask for the management interface.

> **Important:** The DVX System uses the management network to send support data to the Datrium Support portal. The Internet gateway must be on the same subnet as the interface that you use for Data Node management traffic.

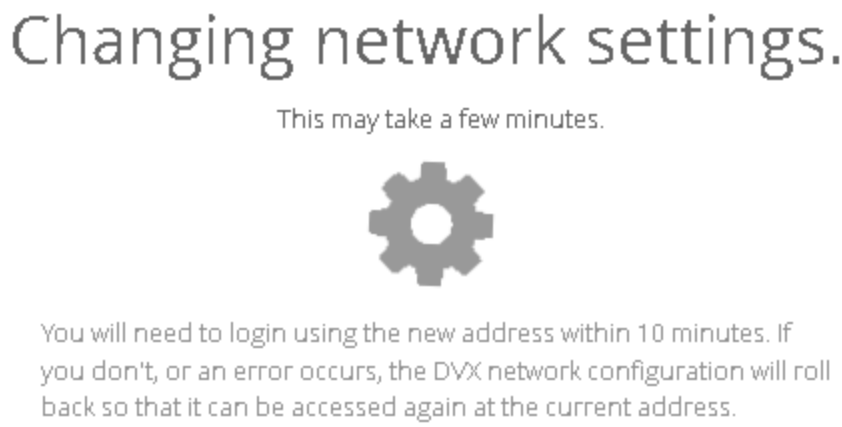


Applying the Network Configuration

After you enter the network configuration data, click on the “Configure network” button. It may take a few minutes to apply the configuration. The zeroconf connection will be disabled. You have 10 minutes to log in again, this time using the management subnet and the management floating IP address. While the DVX System applies the network configuration, the GUI displays the “Changing network settings page.

In order to log in again, disconnect the temporary ethernet cable connection to the eth1 port on the active controller, and connect the configured management interface to your management subnet. Then you can use the management floating IP address to log in over the management subnet.

Changing Network Settings



When the DVX System has applied the network configuration, the GUI displays the “Network changed” page. This page includes a countdown timer that indicates how long you have to log in to commit the configuration.

When you click on either the management floating IP address link or the “Continue” button, the GUI creates a new tab that you use to log in with the new network configuration. When you log in, the DVX System will commit the network configuration, terminate the original connection and disable zeroconf host name access to the Data Node.

> **Important:** To commit the network configuration, you must log in to the Data Node again. You have 10 minutes after you click “Configure network” to log in again. If you do not log in within the 10-minute time period, the DVX System will roll back the network settings.

- If the 10-minute network configuration time period expires, the DVX System will roll back the network settings and you will not be able to log in with the management floating IP address.
- When the 10-minute time period expires, the GUI displays a “Go back” button. If you press “Go back”, the GUI displays the login screen. You must log in again and enter all of the values for initial configuration again.
- If you press “Continue” after the network configuration has been rolled back, it will produce an HTTP error on the tab that was created for the new login. On the original tab, you can press "Go back" to re-apply the network configuration.

If anything goes wrong and you cannot access the Data Node, wait 10 minutes and it should become available again with the zeroconf URL.

vCenter Registration

When you register the vCenter Server, the operation registers the DVX GUI plug-in on the vCenter Server. The vCenter Server will automatically retrieve the plug-in from the Data Node and install it in the Web Client.

vCenter registration includes the following actions:

- Data Node registration – Provides access to the Data Node for DVX System setup on hosts.
- DVX GUI plug-in registration – Supports retrieval of the plug-in from the Data Node for installation on the vSphere Web Client platform.

After you register the Data Node on the VCenter Server, the Server uses the plug-in registration to obtain the DVX GUI plugin from the Data Node for installation on the Web Client.

To perform vCenter registration, you must provide the IP address or DNS name for the vCenter Server and the login credentials for your vCenter account. The account must have administrator privileges.

You must register a vCenter Server so that you can add hosts to the DVX System. You have the option of performing vCenter registration at a later point in time. If you do not register a vCenter Server now, you will have the opportunity to do it the next time you log in to the Data Node. you can use either the Data Node GUI or the DVX CLI to perform vCenter registration.

> **Important:** If you register a vCenter Server that is part of a linked mode group, you must register all vCenter Servers in the group.

When registration is complete, the GUI displays the “Finished” page. Click on the “Continue” button to display the DVX dashboard.

> **Note:** The vCenter Server might not load the plug-in. You must restart the vSphere Web Client service to force the Web Client to load the plug-in. Use the following command(s) to restart the Web Client on vCenter Server Virtual Appliance (vCSA) or on a Windows installation.

vCenter Server / VMware KB article	Command(s)
vCSA Stopping, starting, or restarting vCenter Server Appliance services (2054085)	`service vsphere-client restart`
pre-6.0 Windows vCenter installation How to stop, start, or restart vCenter Server services (1003895)	`services.msc`

6.0 and later Windows vCenter installation
 	
Stopping, starting, or restarting VMware vCenter Server 6.0 services (2109881)
	`service-control --start vsphere-client`
	
	`service-control --stop vsphere-client`

6.5 and later Windows vCenter installation
HTML 5 UI
 	
Stopping, starting, or restarting services in vCenter Server Appliance 6.5 (2147152)
	`service-control --start vsphere-ui`
	
	`service-control --stop vsphere-ui`

For examples, see the Datrium KB article How to restart vCenter Web Client Services.

Configure Data Node and DVX (CLI)

The DVX CLI provides a setup wizard that guides you through the process of configuring the Data Node and DVX System. Before you start the software configuration, make sure you have satisfied the Requirements for DVX Software Configuration. The Data Node ports that you intend to use should be connected to your network. The same ports on both controllers must be connected to the network.

To use the DVX CLI to perform initial configuration of a DVX Node, you can use a direct ethernet connection or a serial port connection. If you use a direct ethernet connection, your client system must have zero configuration software in order to establish the connection with the Data Node.

Network Access for First-Time Data Node Connection

The DVX System supports a zero configuration (zeroconf) connection to the Data Node. The Data Node provides a zeroconf service that uses the Avahi implementation of the zeroconf specification. The Data Node uses the mDNS multicast protocol to support the zeroconf connection.

Requirements for zero configuration access to the Data Node

Your system must have the multicast DNS responder daemon and your system must allow access over UDP port 5353.

Multicast DNS responder software is available on different operating system platforms as part of various software packages.

Windows	You must install responder daemon software. Examples of software that is available for Windows and includes the multicast DNS responder are iTunes and the Apple Bonjour Print Services.
OS X	The responder daemon software is part of Mac Os X.
Linux	You must install the Avahi and nss-mdns packages that are appropriate for

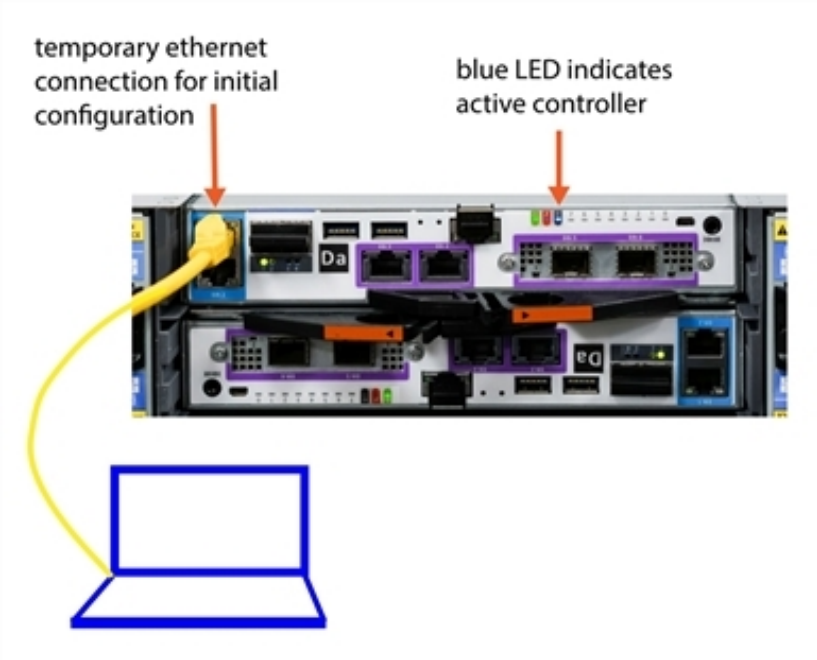
	your particular Linux distribution. The following nss-mdns links might be useful: • http://0pointer.de/lennart/projects/nss-mdns/ • https://launchpad.net/ubuntu/+source/nss-mdns • http://rpmfind.net/linux/rpm2html/search.php?query=nss-mdns It might be necessary to start the Avahi daemon. If your browser cannot resolve the Data Node Zero Configuration URL, use the `avahi-autoipd` command to acquire a link local address. `avahi-autoipd -D network-`*`interface`* `[--force-bind]` Use the `--force-bind` argument only if you cannot bind a link local address to a dedicated interface that is not configured with a routable IP address.

The Data Node uses an IPv4 link-local IP address in the address block 169.254.0.0/16. The operating system on your client system must be able to use the link-local subnet to respond to the Data Node.

Ethernet Connection to the Data Node

For initial configuration, use an Ethernet cable to connect your laptop or other client system directly to the management port on the Data Node. Make sure to connect to the management port on the active controller.

The figure below shows a Data Node that has been connected to the local network. During initial configuration, the temporary connection to the eth1 management port on the active controller provides access for the CLI session.



When you save the network configuration, the DVX System will disable the zeroconf connection. At that time, replace the temporary connection with a connection between the configured management port and the management subnet. Then you can use the management floating IP address to log in over the management subnet.

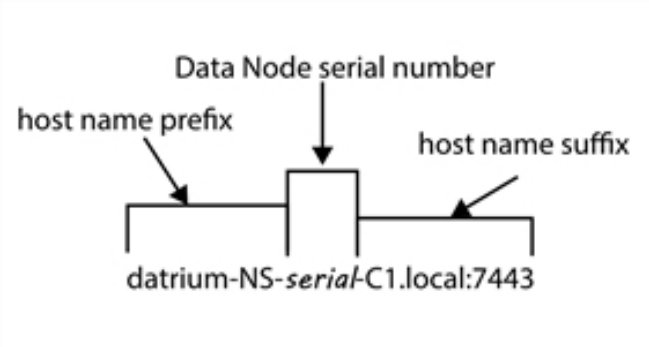
Zero-Configuration Access to the Data Node (SSH)

To use a zero-configuration connection to the Data Node, you construct a host name to identify the Data Node. When you log in, the CLI setup wizard starts automatically.

Data Node Zero Configuration URL

The Data Node zeroconf URL contains the Data Node host name. The host name has three components:

- Host name prefix – “`datrium-NS-`”.
- Data Node serial number – the serial number is on the back of the chassis (see below).
- Host name suffix – Identifies the active controller on the Data Node.



Controller	Host name suffix
1	`-C1.local:7443`
2	`-C2.local:7443`

The Data Node serial number is located on the inside of the left “ear” of the PCM on the left side of the Data Node.

The following string is an example of a zeroconf URL with a Data Node serial number of 000000000000000:

```
https://datrium-NS-000000000000000-C1.local:7443
```

The IP address that is associated with the DVX zero-configuration host name is a random IP address that is not in the local subnet.

It may take a few minutes to establish the zeroconf connection. Ping the Data Node zeroconf URL to determine connectivity.

When you commit your network configuration over the zero configuration connection, the connection is terminated. From that point on, zero-configuration access via the Data Node host name is disabled. To access the Data Node, use the floating point address for the Data Node interface that you are using for management traffic.

If you exit from the wizard without committing the network configuration, zero-configuration access is still available.

Using SSH to Connect to the Data Node

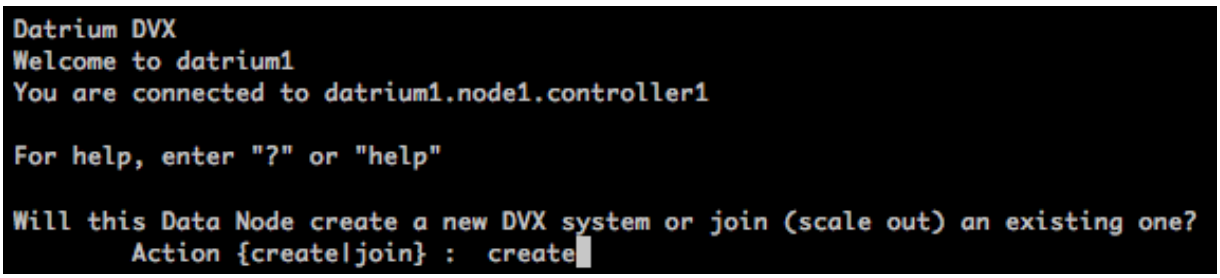
When you create an SSH connection to the Data Node, the connection supports a DVX CLI session. The first time you connect to the Data Node, the CLI wizard starts automatically.

For example, using the serial number 000000000000000, specify the admin account and Data Node zero-configuration host name:

```
ssh admin@datrium-ns-000000000000000-C1.local
```

The default password for the admin account is “datrium#1”. When you login, the DVX CLI will start the Data Node configuration wizard automatically.

> **Tip:** For security, we recommend that you create a password that contains at least 10 characters, including a combination of uppercase and lowercase letters, numbers, and special characters. You can change this password using the DVX CLI `config password set` command.



The wizard gives you the option of creating a new DVX System or joining an existing one. Enter “create” to start the configuration process. For information about adding a Data Node to an existing DVX System, see “Expanding the Data Pool” in the *DVX System Management* manual.

- The wizard will guide you through the setup procedure to configure DVX settings and Data Node network interfaces, and register the DVX GUI plugin with the vCenter Server. If there are suggested or pre-existing values, the wizard will display them in brackets. To use a suggested or pre-existing value, press ENTER. To change it, type in the desired value.

- After network configuration, you will have the opportunity to apply the new settings or to perform network configuration again. After you apply the network settings, you have 10 minutes to commit the network configuration. The commit time window begins when the apply operation begins. If you do not commit within this time window, the DVX System will discard the new settings and revert to the previous configuration.

Type CTRL-C at anytime to exit from the wizard. Use the CLI command “config initial-setup” to invoke the wizard again.

You can continue with the wizard to perform Data Node and DVX configuration. See Network Access for First-Time Data Node Connection.

Serial Port Access for First-Time Connection to the Data Node

> **Important:** After you finish Data Node configuration over the serial port, unplug the serial port cable from the Data Node. Do not leave the serial port cable connected to the Data Node when it is disconnected at the other end as this will produce electrical noise on the Data Node serial port.

Use the serial port cable to connect a laptop (or other computer with a serial port) to the active controller on the Data Node. (Datrium supplies a serial port cable in the Data Node shipping package.) On a new Data Node, although not guaranteed, the top controller should show a blue LED indicating that it is the active controller.

Use the following serial port settings:

Serial port speed	115200
Data bits	8
Stop bit	1

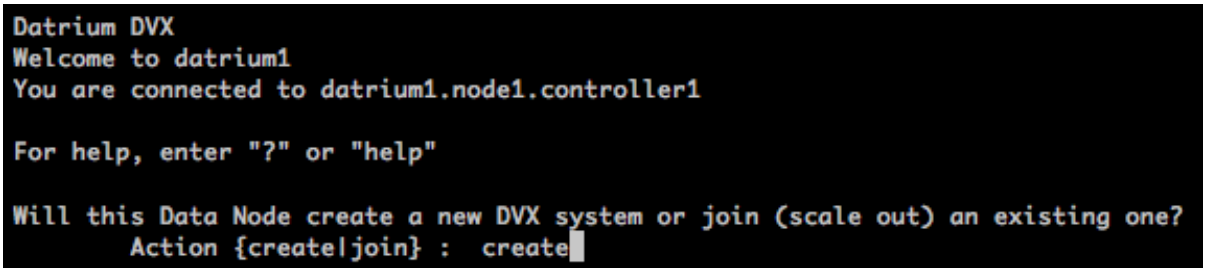
Serial port speed	115200
Parity	None

Data Node Login – Serial Port Connection

After you have established the serial port connection, log in to the Data Node administration account. Use the following credentials:

```
account: admin
password: datrium#1
```

When you login, the DVX CLI will start the Data Node configuration wizard automatically.



The wizard gives you the option of creating a new DVX System or joining an existing one. Enter “create” to start the configuration process. For information about adding a Data Node to an existing DVX System, see “Expanding the Data Pool” in the *DVX System Management* manual.

The wizard will guide you through the setup procedure to configure DVX settings and Data Node network interfaces, and register the DVX GUI plugin with the vCenter Server. If there are suggested or pre-existing values, the wizard will display them in brackets. To use a suggested or pre-existing value, press ENTER. To change it, type in the desired value.

- After network configuration, you will have the opportunity to apply the new settings or to perform network configuration again. After you apply the network settings, you have 10 minutes to commit the network configuration. The commit time window begins when the apply operation begins. If you do not commit within this time window, the DVX System will discard the new settings and revert to the previous configuration.

- Type CTRL-C at anytime to exit from the wizard. Use the CLI command “config initial-setup” to invoke the wizard again.

You can continue with the wizard to perform Data Node and DVX configuration. See Serial Port Access for First-Time Connection to the Data Node.

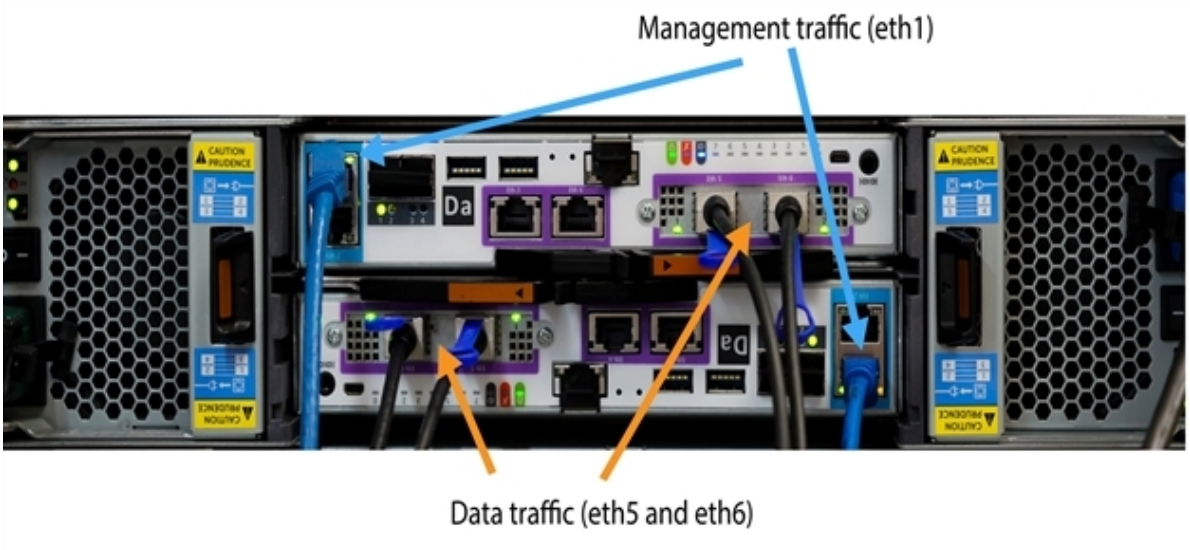
Using the CLI Setup Wizard

The following sections describes a wizard session that is based on the following aspects:

- Static IP address configuration.
- Separate data and management subnets.
- Teamed port configuration for the Data Node data ports.

Separate Data and Management Traffic, Bonded Failover Data Interface

The picture below shows an example of cable connections for this configuration. This example shows teamed port pairs for redundant data traffic (eth3 and eth4, 10Gb SFP+, black cables) and the eth1 1Gb BASE-T interface for management traffic (orange cables).



For information about the DVX network environment, see DVX Network Support.

To perform Data Node and DVX configuration, use the following procedures:

1. DVX System Access and Identification
2. Data Node Network Configuration
3. Register the Data Node with the vCenter Server

After you have completed vCenter Server registration, you can perform Verification and Additional DVX Configuration and then log in to the vSphere Web Client and use the DVX GUI to add hosts to the DVX System.

1. DVX System Access and Identification

During DVX configuration, you can change the admin account password and the DVX name.

The admin account on a new Data Node has the default password `datrium#1`. To change the password, enter the existing password. The wizard will prompt you for a new password and for confirmation.

For security, we recommend that you create a password that contains at least 10 characters, including a combination of uppercase and lowercase letters, numbers, and special characters.

```
DVX SETTINGS

To change the admin account password, type in the current password.
To keep the existing password, press ENTER.

            Current password :
Changing password for admin in datrium1
                New password :
            Confirm password :
Password for admin changed
```

A new Data Node has the default DVX name `datrium#1`. Enter a new name to change it.

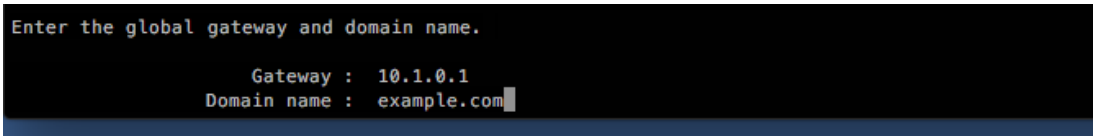
```
Enter the DVX name.

         DVX name [datrium1] :
```

2. Data Node Network Configuration

1. The following example shows the wizard-based sequence for static IP configuration of Data Node interfaces using separate data and management subnets with a bonded failover port configuration for the Data Node data ports.

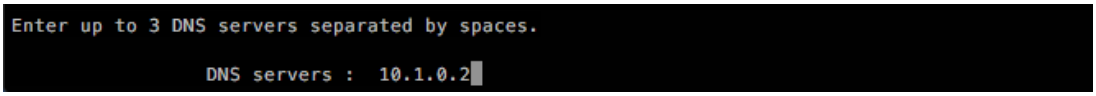
   Enter the gateway IP address and the domain name.



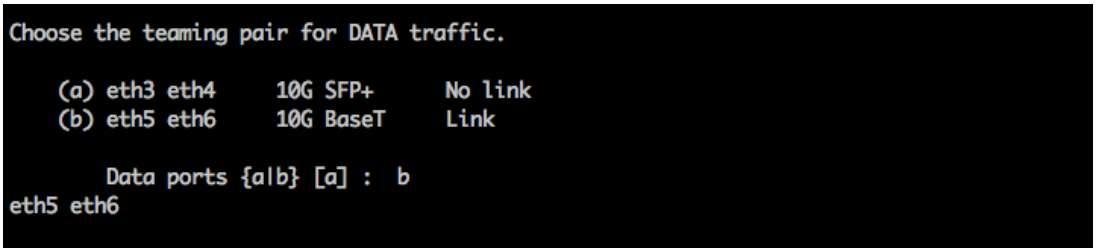
   You must configure a gateway to the Internet so that the DVX System has access to the Datrium Support server at `autosupport.datrium.com`. Make sure that the gateway IP address is on the same subnet as the Data Node interface that you use for management traffic.

   Set the domain name for the Data Node.

2. Enter IP addresses for DNS servers. You can specify up to three DNS servers. Use the space character as a delimiter.



3. You have the choice of SFP+ or 10Gbase-t teamed network interfaces for data traffic. The following example shows that the 10Gbase-t interfaces have active links. Enter “b” to select the active eth5 and eth6 ports for data traffic. The interface/port selection represents the same port(s) on both controllers on the Data Node. When you apply the configuration, the DVX System configures the same port(s) on both controllers to support controller failover.



The following table shows the interface types for the data ports:

Configuration	Interface Specification	Interface Type
Teamed pair (data traffic)	eth3 eth4	10Gb SFP+ (direct attach or optical)
	eth5 eth6	10Gb BASE-T RJ45 Ethernet

4. You must provide five IP addresses and a netmask for the teamed data interface.

   The DVX System uses the floating IP address for access to the data interface. If there is a network failover or a controller failover, the floating IP address is automatically assigned to the active port.

   You must supply two data IP addresses for each controller (Controller1 and Controller2).

   The subnet mask is the dot-decimal representation of the network mask for the data interface.

```
Enter the DATA IP addresses and subnet mask.

                Floating IP :  192.0.0.106
           Controller1.eth5 :  192.0.0.107
           Controller1.eth6 :  192.0.0.108
           Controller2.eth5 :  192.0.0.109
           Controller2.eth6 :  192.0.0.110
                Subnet mask :  255.255.255.0
```

5. Enter “a” to select the eth1 management interface.

```
Choose the port or teaming pair for MGMT traffic.

   (a) eth1          1G BaseT    Link
   (b) eth2          1G BaseT    No link
   (c) eth1 eth2     (teaming pair)

     Mgmt ports {a|b|c} [c] :  a
eth1
```

   An interface selection represents the same port(s) on both controllers on the

Data Node. When you execute the command, the DVX System configures the same ports on both controllers to support controller failover.

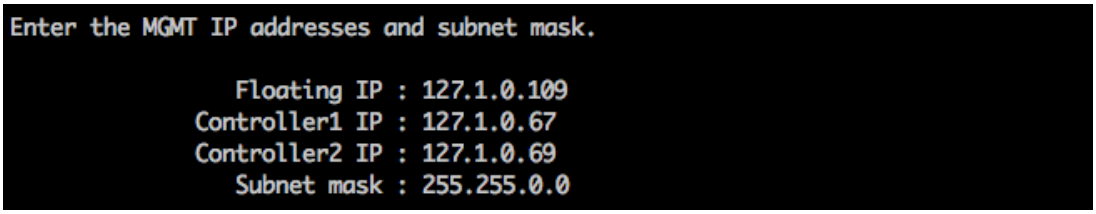
> **Important:** The DVX System uses the management network to send support data to the Datrium Support portal. The Internet gateway must be on the same subnet as the Data Node interface that you use for management traffic.

6. You must provide three IP addresses and a netmask for the management interface.

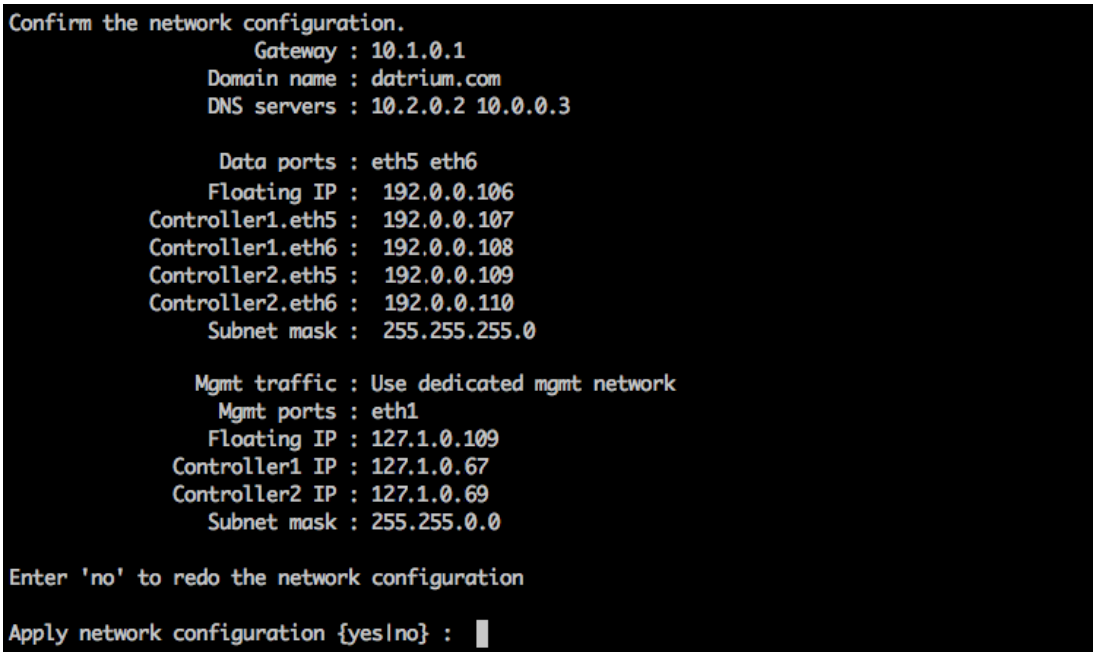
   The DVX System uses the floating IP address for access to the management interface. If there is a network failover or a controller failover, the floating IP address is automatically assigned to the active port. Use the management interface floating IP address when you create a DVX CLI session.

   You must supply IP addresses for both controllers (Controller1, Controller2).

   The subnet mask is the dot-decimal representation of the network mask for the management interface.



7. After you enter the management interface settings, the wizard displays the entire network configuration for confirmation and prompts you to apply and then commit the configuration. Enter “yes” to apply the configuration. The apply operation may take several minutes. Enter “no” to repeat the network configuration.



After you apply the network settings, you have 10 minutes to commit the network configuration. The commit time window begins when the apply operation begins. The zeroconf connection will be disabled. You have 10 minutes to log in again, this time using the management subnet and the management floating IP address. If you do not commit within this time window, the DVX System will discard the new settings and revert to the previous configuration.

In order to log in again, disconnect the temporary ethernet cable connection to the eth1 port on the active controller, and connect the configured management interface to your management subnet. Then you can use the management floating IP address to log in over the management subnet.

3. Register the Data Node with the vCenter Server

When you register the vCenter Server, the operation registers the DVX GUI plug-in on the vCenter Server. The vCenter Server will automatically retrieve the plug-in from the Data Node and install it in the Web Client.

vCenter registration includes the following actions:

- Data Node registration – Provides access to the Data Node for DVX System setup on hosts.
- DVX GUI plug-in registration – Supports retrieval of the plug-in from the Data Node for installation on the vSphere Web Client platform.

After you register the Data Node on the vCenter Server, the Server uses the plug-in registration to obtain the DVX GUI plugin from the Data Node for installation on the Web Client.

To perform vCenter registration, you must provide the IP address or DNS name for the vCenter Server and the login credentials for your vCenter account. The account must have administrator privileges.

Important: If you register a vCenter Server that is part of a linked mode group, you must register all vCenter Servers in the group.

Note: The vCenter Server might not load the plug-in. You must restart the vSphere Web Client service to force the Web Client to load the plug-in. Use the following command(s) to restart the Web Client on vCenter Server Virtual Appliance (vCSA) or on a Windows installation:

vCenter Server / VMware KB article	Command(s)
vCSA Stopping, starting, or restarting vCenter Server Appliance services (2054085)	`service vsphere-client restart`
pre-6.0 Windows vCenter installation How to stop, start, or restart vCenter Server services	`services.msc`

vCenter Server / VMware KB article	Command(s)
(1003895)	

6.0 and later Windows vCenter installation
 	
Stopping, starting, or restarting VMware vCenter Server 6.0 services (2109881)
	`service-control --start vsphere-client`
	
	`service-control --stop vsphere-client`

6.5 and later Windows vCenter installation HTML 5 UI
 	
Stopping, starting, or restarting services in vCenter Server Appliance 6.5 (2147152)
	`service-control --start vsphere-ui`
	
	`service-control --stop vsphere-ui`

For examples, see the Datrium KB article How to restart vCenter Web Client Services.

Next: Verification and Additional DVX Configuration.

Verification and Additional DVX Configuration

After you complete network configuration and vCenter registration, use the following procedures to verify the network configuration and perform additional DVX configuration.

- Verify Gateway Access to the Support Server (DVX CLI)
- Verify Floating IP Addresses

Additional Configuration:

- Additional Configuration – DVX GUI
- Additional Configuration – DVX CLI

Verify Gateway Access to the Support Server (DVX CLI)

To verify access to the Datrium Support Server, use the DVX CLI.

Log in to the Data Node and use the DVX CLI command `support test`.

```
ssh admin@mgmt-floating-ip
admin@mgmt-floating-ip's password:

>> support test
HTTP connection Test successful
```

If there is a problem, you might see an HTTP error.

```
datrium1.controller1>> support test
HTTP connection to support server failed due to bad
HTTP status code 404
```

If you are using a firewall, make sure that you have configured access appropriately.

If you are using an HTTP proxy in your environment, you must configure the web proxy to identify the proxy server and port for HTTP access.

- DVX GUI – Configure Access to a Web Proxy and Save the Configuration
- DVX CLI – Configure Access to a Web Proxy

If you are using the management interface on the Data Node, the DVX System uses that interface for access to the gateway. If you disable the management interface, you must reconfigure the gateway so that it is on the data subnet.

Verify Floating IP Addresses

To verify the Data Node network interface configuration and support for DVX HA, execute a Data Node failover and ping the data and management floating IP addresses. In the following procedure, you will ping the Data Node twice. Ping the Data Node from another machine on your network. If the Data Node does not respond to a ping operation, you must verify your switch configuration.

1. From a remote system, verify initial connectivity.

   ```
   ping mgmt-floating-ip-addr
   ping data-floating-ip-addr
   ```

2. Use the management floating IP address to log in to the DVX CLI on the Data Node and perform a failover.

   ```
   nodes failover
   ```

3. From a remote system, verify network support for the floating IP addresses.

   ```
   ping mgmt-floating-ip-addr
   ping data-floating-ip-addrfloating-ip-addr
   ```

4. Log in to the Data Node again and restore the initial configuration.

   ```
   nodes failover
   ```

Additional Configuration – DVX GUI

Use the following procedures to finish the DVX configuration.

- Set Up Email Alerts
- Configure Access to an NTP Time Server
- Configure Access to a Web Proxy and Save the Configuration

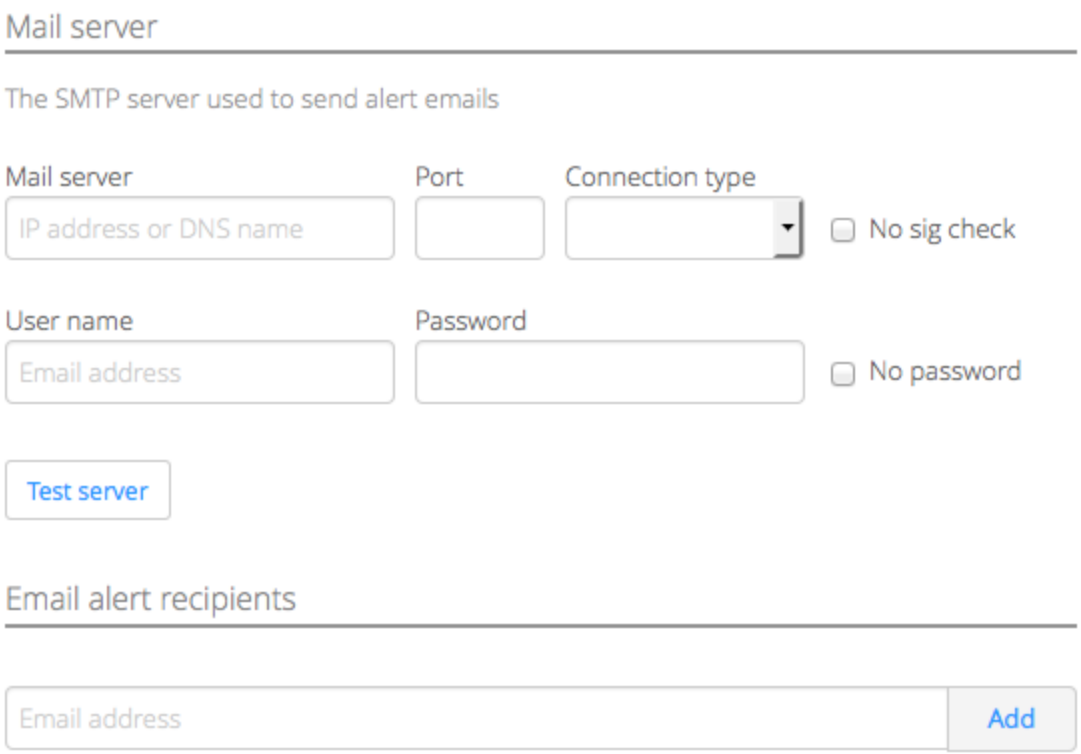
Set Up Email Alerts

The DVX System requires access to a mail server to send an alert to a user. To configure email support for DVX System alerts, you identify the SMTP server and specify whether the SMTP server will use encryption.

- To identify the mail server, use an IP address or a DNS name.
- The DVX System uses port 25 as the default port for SMTP communication. Enter a different port if necessary.
- By default, the DVX System uses unencrypted SMTP for email transmission. To use encrypted email transmission, you must specify either “SMTPS” or “TLS” for the connection type. If you specify “SMTPS”, the DVX System will use SSL encryption.
- Specify the user name and password for the account that will be used to connect to the mail server. Alert email messages will use this user name for the “From” field value.
- Select “No sig check” to bypass certificate validation. This is intended for use with a mail server that uses self-signed certificates. This creates a security vulnerability. Use this capability with care.
- Enter email address(es) for the alert recipient(s).

After you save the configuration, click on the “Test server” button to send a test email. The GUI displays a field that you use to enter the test email recipient.

DVX GUI – Email Alerts

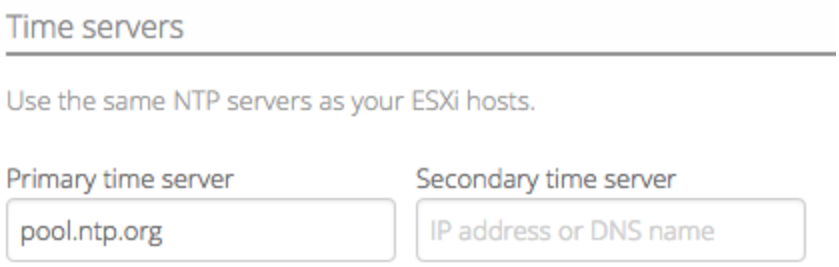


If you are using a Google Gmail server with 2-Step Verification, the Gmail server might prevent login from the DVX Data Node. If this is the case, when you test the DVX mail server configuration (Test server) you will see an error. The Gmail server does not recognize the DVX Data Node. To solve this problem, use an App password. See https://support.google.com/accounts/answer/185833?hl=en.

Configure Access to an NTP Time Server

The DVX System uses an NTP time server to synchronize the system. You can set a primary time server and an optional secondary time server. The DVX System uses pool.ntp.org as the default primary time server.

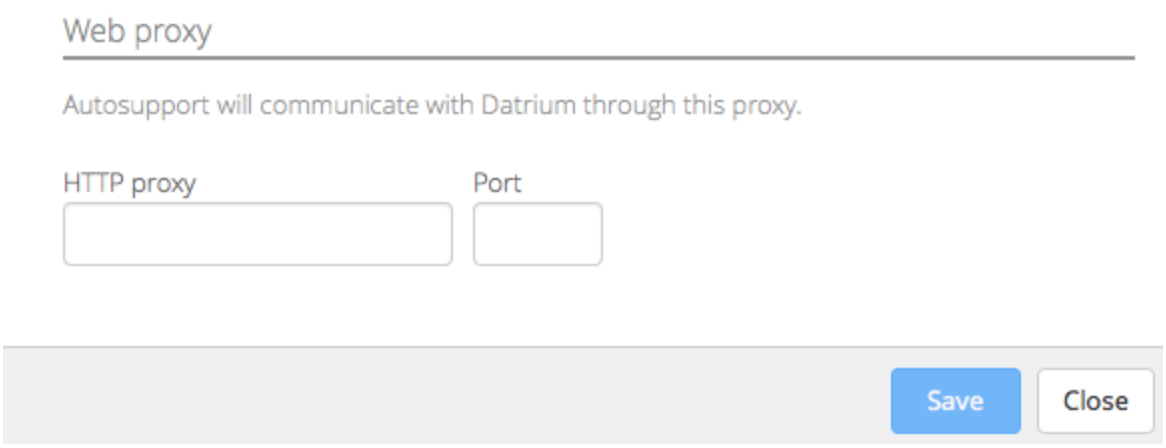
DVX GUI – NTP Time Server Configuration



Configure Access to a Web Proxy and Save the Configuration

If you are using an HTTP proxy server in your environment, you must identify the proxy IP address and port for the DVX System. The DVX System will use the proxy to communicate with the Datrium Support Server.

DVX GUI - Web Proxy Configuration



After you finish entering configuration data, save the configuration.

Additional Configuration – DVX CLI

To complete Data Node configuration, you must perform the following additional configuration tasks:

- Configure Access to a Web Proxy
- Set Up Email Alerts
- Configure Access to an NTP Time Server

After you complete the additional configuration, Terminate the CLI Session.

Configure Access to a Web Proxy

If you are using an HTTP proxy server in your environment, use the web-proxy set command to identify the proxy IP address and port for the DVX System.

```
config web-proxy set --proxy-server proxyServerIP
                     --proxy-port portNum
```

Use the following command to display the HTTP proxy configuration:

```
config web-proxy show
```

Set Up Email Alerts

Use the following commands to configure access to a mail server and identify personnel who will receive email about critical events.

```
1) config mail-server set [--connection-type SMTP |
SMTPS | TLS]
                           --host ipAddress | dnsName
                          [--port portNum ]
                           --user userName
                          [--passwd password ]
                          [--no-sig-check]
                          [--test]
```

- The default connection type is unencrypted SMTP. To use encrypted

email transmission, you must specify either `smtps` or `tls` with the `--connection-type` argument. If you specify `smtps`, the DVX System will use SSL encryption. To maintain email encryption, you must specify one of the encryption connection types each time you invoke the mail-server set command.

- To identify the mail server, use the `--host` argument. You can specify an IP address or a DNS name.
- The DVX system uses port 25 as the default port for SMTP communication. To use a different port on the mail server, specify the `--port` argument.
- The `-user` argument specifies the account name that will be used to connect to the mail server. Alert email messages will use this account name for the "From" field value.
- The `-passwd` argument specifies the mail server account password.
- Use the `-no sig check` argument to bypass certificate validation. This is intended for use with a mail server that uses self-signed certificates. This creates a security vulnerability. Use this argument with care.
- Use the `-test` argument to send a test email to the specified server. The configuration is applied only if the test is successful.

2) `config alert-recipients add mailto:`*`user@host`*

- When you configure an alert recipient, you must use the "mailto:" prefix with the email address.

Use the following command to display the mail server configuration:

```
config mail-server show
```

Use the following command to verify the mail server configuration. If you do not specify a subject or body, the DVX System will supply default subject or body text.

```
config mail-server test --email-address emailAddress
                        [--subject subjectText ]
                        [--body bodyText ]
```

If you are using a Google Gmail server with 2-Step Verification, the Gmail server might prevent login from the DVX Data Node. If this is the case, when you test the DVX mail server configuration (config mail-server test) you will see an error similar to the following:

```
Test failed. [...] <https://ac-
counts.google.com/ContinueSignIn?[...]>
Please log in via your web browser and [...] then try
again.
Learn more at [...] https://sup-
port.google.com/mail/answer/78754 [...]
```

The Gmail server does not recognize the DVX Data Node. To solve this problem, use an App password. Seehttps://support.google.com/accounts/answer/185833?hl=en.

Configure Access to an NTP Time Server

Use the following command to configure access to NTP time servers for DVX System time synchronization.

```
config time-server set --primary-time-server-ip
primaryTimeServerIP
                       [--optional-time-server-ip
optionalTimerServerIP]
```

The DVX System uses pool.ntp.org as the default primary time server.

Use the following command to display the time server configuration:

```
config time-server show
```

Terminate the CLI Session

If you will be using DVX Additional Configuration – DVX CLI, enable encryption before logging out of the CLI session.

Log out from the DVX CLI session.

```
>> exit
Connection to example.datrium.com closed.
```

If you are using a serial port connection, terminate the screen session:

```
screen -X -S session_id
```

> **Important:** After you finish Data Node configuration over the serial port, unplug the serial port cable from the Data Node. Do not leave the serial port cable connected to the Data Node when it is disconnected at the other end as this will produce electrical noise on the Data Node serial port. It is recommended that you keep the serial port cable in a safe place.

Enable Blanket Encryption

To enable encryption, use the DVX CLI. Use ssh to log in to the Data Node:

```
ssh admin@mgmt-floating-ip
admin@mgmt-floating-ip's password:
```

Use the CLI command “datastores encryption enable” to enable data encryption on the DVX System.

```
datastores encryption enable
```

The first time you enable encryption, the CLI prompts you for two encryption passwords.

You must save the encryption access passwords. The DVX System secures the passwords but you cannot recover the passwords. If you set the startup mode to lock and then lose the encryption access passwords:

- You will not be able to access your data after restarting or upgrading the Data Node.
- You will not be able to change the encryption settings.

For security, we recommend that you create a password that contains at least 10 characters, including a combination of uppercase and lowercase letters, numbers, and special characters.

When encryption is enabled, all new data is encrypted and one of the encryption passwords is required to use the encryption commands. The DVX System encrypts data on Compute Node flash, the Data Node(s), and on the network connection between the Data Node(s) and DVX Compute Nodes.

For more information about Blanket Encryption, see “Blanket Encryption” in the *DVX System Management* manual and the description of the `datastores encryption` commands in the *DVX Command Line Interface* manual.

User management

By default, the DVX system has a predefined administration account used to log in to DVX UI or CLI.

- account: `admin`
- password: `datrium#1`

If you have Active Directory (AD) configured in your network, you can use the DVX CLI to configure your AD server so that your users can sign in to the DVX GUI using their active directory credentials.

You can map users from a specific AD group to the 'admin' role in the DVX system ('`DA_ADMIN`'). All AD users who are mapped to the DVX admin role will be considered DVX administrators and will have full access to all features of the DVX system. Any associated operations done by the user will be logged as user-initiated DVX system events.

Configure Active Directory

To configure your AD server for use with the DVX system, use the `active-directory set` CLI command.

Format:

```
config active-directory set [--domain DOMAIN]
                        [--primary-dc-name
PRIMARYDCNAME]
                        [--primary-ldap-port
PRIMARYLDAPPORT]
                        [--secondary-dc-name
SECONDARYDCNAME]
                        [--secondary-ldap-port
```

```
SECONDARYLDAPPORT]
                          [--output-format OUTPUT_FORMAT]
```

- `--domain`. Specifies where the domain where the Active Directory server is located.
- `--primary-dc-name`. The name of the primary Domain Controller to use for LDAP communication.
- `--secondary-dc-name`. The name of the secondary Domain Controller to use for LDAP communication.
- `--primary-ldap-port`. The primary DC Port used for LDAP communication. If left empty, will default to port 389
- `--secondary-ldap-port`. Secondary DC Port used for LDAP communication. If left empty, this will default to port 389.

For example:

```
config active-directory set --domain
mycompany.domain.com --primary-dc-name my-colo-dc-00 -
-secondary-dc-name my-other-colo-dc-01
```

Disable Active Directory Configuration

To disable your DVX Active Directory configuration, use the `active-directory unset` CLI command.

Format:

```
config active-directory unset [--output-format json |
default]
```

Show Active Directory Configuration Settings

To display the current DVX Active Directory configuration settings, use the `active-directory show` CLI command.

Format:

```
config active-directory show [--output-format json |
default]
```

Configure RBAC for DVX

You can use the `rbac add-active-directory-group` CLI command to add an AD group from your AD system and associate it with the DVX `DA_ADMIN` role. Any users that belong in the mapped the selected AD group will be able to log in to the DVX GUI and perform all operations. Additionally, any operations will be associated with the logged-in user as DVX audit events.

> **Note:** AD user names must be in User Principal Name (UPN) format. Additionally, the backslash format is not supported for user names.

> **Note:** The AD feature requires at least one RBAC AD group-role set. If no group is added, then login will not be enabled for AD users.

Format:

```
config rbac add-active-directory-group
                          --group GROUP
                           --roles ROLES [ROLES ...]
                          [--output-format OUTPUT_
FORMAT]
```

- `--group`. The name of the Active Directory group to associate with the DVX 'admin' role (`DA_ADMIN`). To perform this operation, you need a valid set of AD credential to add the group. This flag allows you to add one AD group at a time.
- `--roles`. The DVX role to associate with your AD group. Currently, only the single `DA_ADMIN` role is supported, which gives associated users all permissions to perform all operations in the DVX system. Setting `--roles` is mandatory.

Remove an AD Group from the DVX System

You can use the `rbac remove-active-directory-group` to remove an AD group that was associated with the DVX `DA_ADMIN` role, and will disallow users belonging to that

group from accessing and using the DVX system.

Format

```
config rbac remove-active-directory-group --group
GROUP
                                                --roles
ROLES [ROLES ...]
                                               [--output-
format OUTPUT_FORMAT]
```

- `--group`. The name of the Active Directory group you want to remove from the DVX RBAC configuration. You need a valid set of AD credential to remove the group. Once removed, users belonging to this group will no longer have access to the DVX system.
- `--roles`. Optional. Currently, only the single `DA_ADMIN` role is supported. If no role is given, then the group will be removed completely; otherwise. only the given role will be deleted.

Show RBAC Settings

You can use `rbac show` CLI command to display the mapping between the local DVX user (DA_ADMIN) and your AD groups.

Format:

```
config rbac show [--output-format json | default]
```

Upload a custom certificate

By default, the DVX system uses a default self-signed SSL certificate for browser authentication. If you want to provide your own certificates to access to DVX through a web browser, or for the DVX GUI vCenter plug-in, you can use the DVX UI to import a custom certificate into the DVX system.

> **Note:** If you want to use the DVX system's default self-signed certificate, you can also use this feature to regenerate the default self-signed certificate.

The DVX system supports certificate and key files that use either the `.pem` or `.crt` file extension.

Before you upload a custom certificate, make sure you have the following:

- The floating management Full Qualified Domain Name (FQDN) that is mapped to the DVX management floating IP address, as configured in DNS.
- A public x.509 full chain file that contains everything from the root to the owner's public key.
- A private x.509 key associated with the certificate.

The process of uploading a custom certificate requires performing the following tasks:

1. Verify the certificates
2. Unregister all vCenters associated with the DVX system.
3. Upload the new custom certificate.
4. Clear the old certificate from your browser.
5. Re-register the previously unregistered vCenters.
6. Optional: Regenerate default certificate

Verify the Certificates

Before you upload new custom SSL certificates to the DVX System, verify that the certificates are valid.

Also, ensure that the public key chain certificate is uploaded to the DVX System in the reverse order (which is common with Windows based cert tools), or the DVX System will reject any such certificates.

> **Note:** Self-signed root certificates are not supported.

> **Note:** These instructions are for Linux systems. For more information about verifying certificates on a Windows system, see Checking the certificate trust chain for an HTTPS endpoint.

To verify customer certificates before upload:

1. Run this command on a Linux system where you have the certs to verify that the public certificate and its chain of certificates are valid:

   ```
   openssl verify my_publickey_chain.pem
   ```

2. The results state `OK` if the certificate is valid.
3. To compare and verify the public and private keys, copy the public key pair of the chain certificate to a separate file (the chain must only be the final item in the certificate). You should have this file from before you created the chain.
4. Run the following command to get the public signature of the file:

   ```
   openssl x509 -pubkey -in my_publickey.pem -noout
   ```

5. Then compare this with the public signature of the private key:

   ```
   openssl pkey -pubout -in my_privatekey.pem -passin pass:
   ```

6. The output of the previous commands must match exactly for the certificate to be valid.

2. Unregister vCenters from your DVX system

To unregister vCenters from your DVX system, use the following DVX CLI command:

```
config vcenter unregister ipAddr | dnsName
     [--user userName]
     [--password password]
     [--force]
```

Use the `--force` argument to remove the registration from the DVX System if the unregister operation fails on the vCenter Server. This might be necessary for a number of reasons – the vCenter Server is temporarily or permanently unavailable, the DVX GUI plug-in was removed from the vCenter Server or, the vCenter Server was re-initialized.

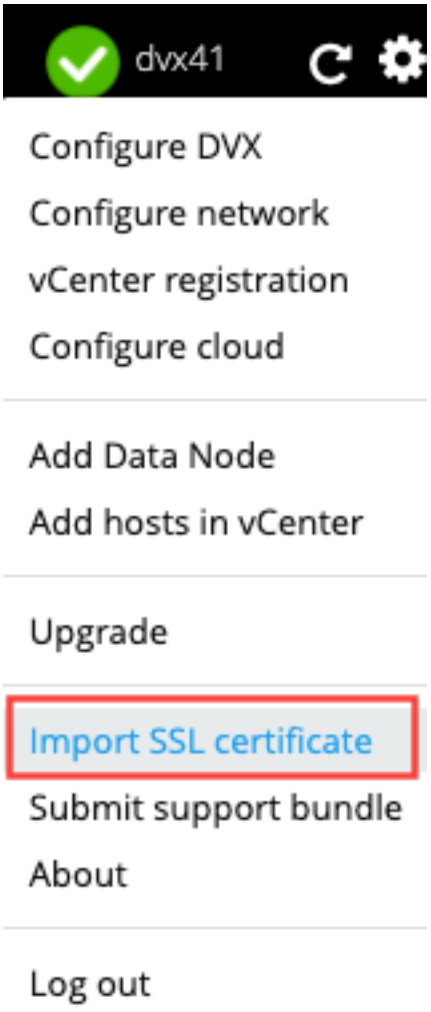
When you first registered the Data Node with the vCenter Server, the DVX System registered a certificate with the vCenter Server for future access. If that certificate was removed, for example if the vCenter database was reinitialized, then you have to supply the user name and password credentials to *remove* the vCenter registration.

When you use this argument, the DVX System will remove the vCenter association on the Data Node.

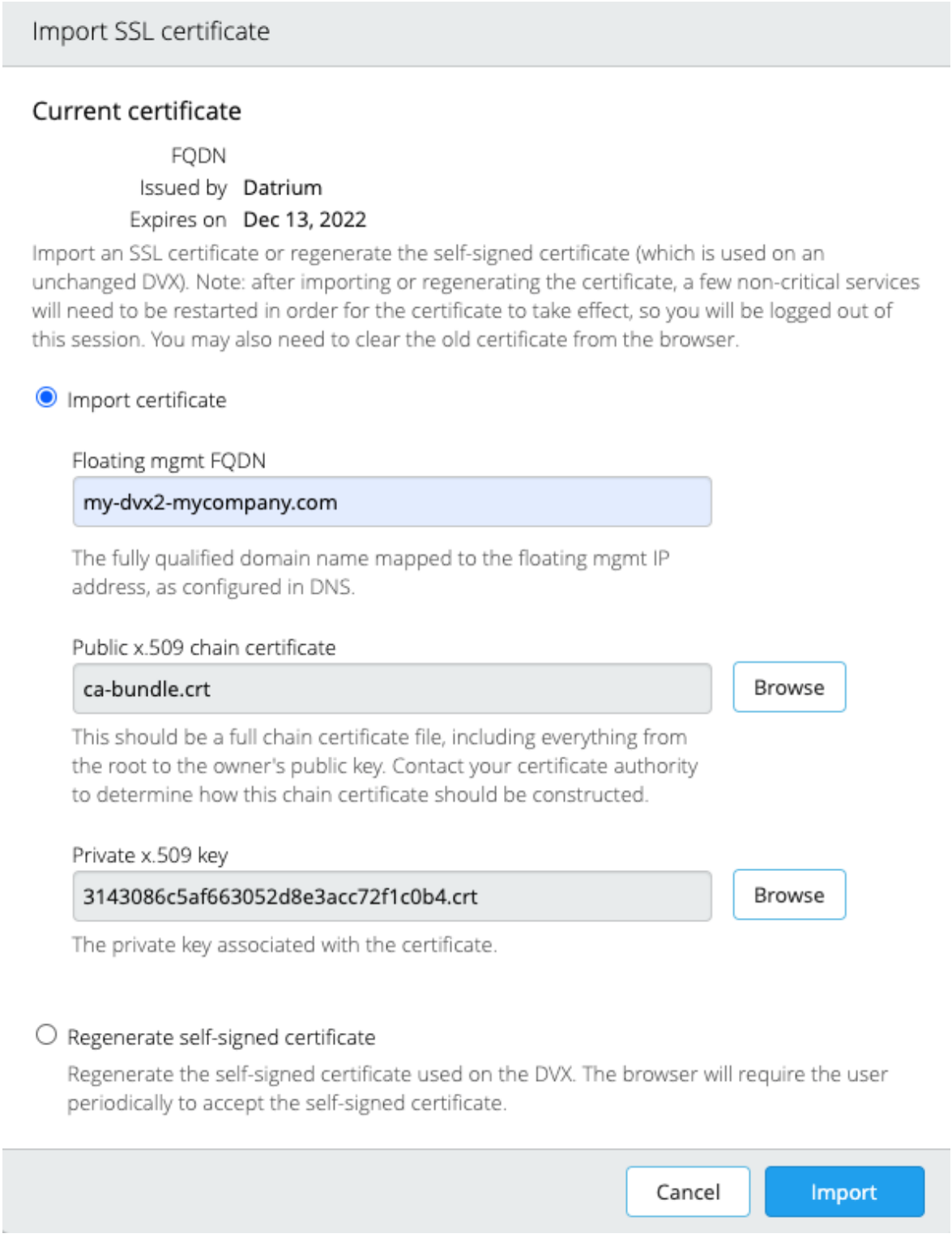
3. Upload a custom certificate

To upload a custom certificate:

1. In the DVX GUI, from small gear icon menu in the upper right of the GUI, select Import SSL certificate.



2. In the Import SSL certificate dialog, select 'Import certificate'.



3. In the dialog, enter the floating management FQDN (the fully qualified domain name mapped to the DVX floating IP address).
4. Click **Browse** to select the public x.509 chain certificate file. This file should include the full chain certificate information, including the root to the owner's public key.
5. Click **Browse** to select the private x.509 key associated with the certificate.
6. Optional: If you only want to regenerate the DVX default certificate, select the 'Regenerate self-signed certificate' option.
7. Click **Import**.

4. Clear old certificate from browser

Next, before you re-register your vCenters with the DVX system, you need to clear the old DVX certificate that was being used for your browser. The default certificate provided by the DVX system is named '*.datrium'.

How you clear the old certificate depends on your computer operation system (Mac OS or Windows) and browser (Chrome or Firefox).

Mac OS

To clear the old Datrium certificate on Mac OS, open the Keychain Access app and search for '*.datrium'. Then, you can right-click the certificate and delete it.

Windows - Chrome

For Chrome browser on Windows, go to the browser's Settings, then select Security and Privacy → Advanced → Manage Certificates. In the Certificates dialog, select the '*.datrium' certificate and click **Remove**.

Windows - Firefox

For Firefox browser on Windows, go to the browsers Options, then select Privacy and Security → Security → Certificates, and then click View Certificates. Scroll in the list of certificates until you find the '*.datrium' certificate, and then click **Delete or Distrust**, and then click **OK**.

5. Re-register vCenters with the DVX System

To register vCenters with DVX system that you previously unregistered, use the following DVX CLI command:

```
config vcenter register ipAddr | dnsName
    [--user userName
    [--password password]
    [--force]
```

- Specify the vCenter Server IP address or DNS name, the vCenter Server account name, and if required, the account password.
- Specify `--force` to ignore the vCenter version. Intended for use by Datrium personnel. If you use this argument to register the Data Node with an unsupported version of vCenter, the DVX plug-in might not work.
- If the Data Node is running the latest version of Datrium software, this command also updates the DVX GUI plug-in registration on the vCenter Server.

Optional: Regenerate a self-signed certificate

If you are not using your own custom SSL certificate and would like to use the DVX default certificate, you can regenerate that certificate at any time.

To regenerate a self signed certificate:

1. In the DVX GUI, from small gear icon menu in the upper right of the GUI, select Import SSL certificate.
2. In the Import SSL certificate dialog, select Regenerate self-signed certificate'.
3. Click **Regenerate**.
4. Click **Close**.

DVX Network Support

The following sections provide information about the DVX network environment. This information is useful when performing Data Node network configuration.

The DVX System supports both controller failover and network failover capabilities. You must connect cables to the set of ports that will support controller failover and your network topology.

- The Data Node operates as an HA capable system. When you configure an interface, it represents the same port(s) on both controllers in the Data Node. You must connect cables to the same ports on both controllers.
- The Data Node supports adaptive pathing over teamed data ports. The teamed ports support aggregate bandwidth. If there is a network failure, the DVX System will continue to use the remaining port(s).

  You can configure one set of teamed data interfaces on a Data Node – SFP+, SFP28, or
  10G BASE-T – according to the Data Node model:

Data Node Model	SFP+, SFP28	10G BASE-T
D12x4	teamed 2x10G ports	teamed 2x10G ports
D12x4B 4x10G	teamed 2x10G ports or teamed 4x10G ports	teamed 2x10G ports
D12x4B 2x25G D12x4C 2x25G D12x10D 2x25G F24x2B 2x25G F24x2D 2x25G	teamed 2x10/25G ports	teamed 2x10G ports

  You must connect cables to all of the ports in the interface team, and to the

corresponding ports on the second controller. The Data Node data interfaces must be on the same subnet as the Compute Nodes for which they will provide data services. For more information about using teamed data ports on the Data Node, see Network Port Redundancy.

- For management traffic to the Data Node, you configure either one or both 1G interfaces. Paired 1G interfaces support active/passive failover operation. You must connect cables to the same ports on both controllers.

Data and Management Subnets

The DVX System supports network environments that use separate subnets for data and management traffic. The Data Node uses 10G or 25G ports for data traffic and a 1G port for management traffic.

- *Data traffic* includes all communication between the Data Node and the DVX Hyperdriver on an ESXi host.
- *Management traffic* includes Datrium Support traffic, DVX GUI and CLI traffic.

Datrium Support traffic requires a gateway for access to the Datrium Support Portal.

Data Node Network Ports

The following sections describe the network ports for the different controller types.

For information about monitoring link activity, see Network Port Status , "Network Port Status" in the DVX System Management guide.

2x25G Data Node Ports: D12x4B, D12x4C, D12x10D and F24x2B, F24x2D

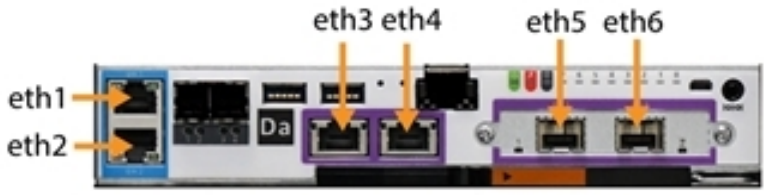
The D12x4B, D12x4C, D12x10D, F24x2B, F24x2D 2x25G Data Nodes support 10G or 25G data traffic.

- To configure the data interface, you select a teamed pair of interfaces of the same connection type – 10BASE-T (eth3+eth4) or SFP+/SFP28 (eth5+eth6; these interfaces

support 10G or 25G traffic).

- To configure the management interface, you select a single interface (eth1 or eth2) or the bonded pair of interfaces (eth1+eth2).

The following table shows the port names and types. Ports are referenced by interface name – eth1..eth6. The port names are shown for controller 1. Controller 2 is turned upside down in the chassis.



CLI Port Name	GUI Port Name	Port Type
node1.controller1.eth1 node1.controller1.eth2	Controller 1 Eth 1 Controller 1 Eth 2	1G RJ45 Ethernet. Used as management ports for the DVX GUI and CLI, and for Datrium Support remote access.
node1.controller1.eth3 node1.controller1.eth4	Controller 1 Eth 3 Controller 1 Eth 4	10G BASE-T RJ45 Ethernet ports used as data ports.
node1.controller1.eth5 node1.controller1.eth6	Controller 1 Eth 5 Controller 1 Eth 6	10G SFP+/25G SFP28 ports used as data ports. These ports accept direct attach twin axial copper connections or optical connections. The SFP interfaces support a data rate according to the capabilities of the switch and the cable that connects the Data Node to it. To support speeds up to 25G with twin-axial copper connections, both the cable and switch must be rated for 25G traffic. If either the cable or switch operates at 10G, the Data Node will

		operate at 10G. Datrium offers 10G/25G dual speed optical transceivers as an option for these 25G-capable Data Nodes.

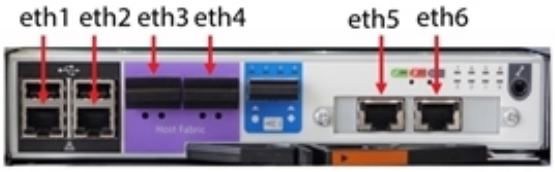
4x10G Data Node Ports: D12x4C

The D12x4C 4x10G Data Node support 10G data traffic.

- To configure the data interface, you select a team of interfaces of the same media type – 10BaseT (eth3+eth4) or SFP+ (eth5+eth6, eth7+eth8, or eth5+eth6+eth7+eth8).
- To configure the management interface, you select a single interface (eth1 or eth2) or the bonded pair of interfaces (eth1+eth2).

The following table shows the port names and types. Ports are referenced by interface name – eth1..eth8. The port names are shown for controller 1. Controller 2 is turned upside down in the chassis.

CLI Port Name	GUI Port Name	Port Type
node1.controller1.eth1 node1.controller1.eth2	Controller 1 Eth 1 Controller 1 Eth 2	1G RJ45 Ethernet. Used as management ports for the DVX GUI and CLI, and for Datrium Support remote access.
node1.controller1.eth3 node1.controller1.eth4	Controller 1 Eth 3 Controller 1 Eth 4	10G BASE-T RJ45 Ethernet ports used as data ports.

node1.controller1.eth5 node1.controller1.eth6 node1.controller1.eth7 node1.controller1.eth8	Controller 1 Eth 5 Controller 1 Eth 6 Controller 1 Eth 7 Controller 1 Eth 8	10G SFP+ ports used as data ports. These ports accept direct attach twin axial copper connections or optical connections. When you use the SFP+ ports, you can use one of the following combinations of these ports: eth5+eth6 eth7+eth8 eth5+eth6+eth7+eth8 Datrium offers 10G optical transceivers as an option for these 10G Data Nodes.
		
CLI Port Name	**GUI Port Name**	**Port Type**
node1.controller1.eth1 node1.controller1.eth2	Controller 1 Eth 1 Controller 1 Eth 2	1G RJ45 Ethernet. Used as management ports for the DVX GUI and CLI, and for Datrium Support remote access.
node1.controller1.eth3 node1.controller1.eth4	Controller 1 Eth 3 Controller 1 Eth 4	10G SFP+ ports used as data ports. The ports require Datrium-supplied adapters that accept the copper cables or optical modules. (Melanox Copper/Direct-Attach cables or Melanox SFP+ 10G BASE-SR optical module.)
node1.controller1.eth5	Controller 1 Eth 5	10G BASE-T RJ45 Ethernet ports used as data ports. If management interfaces are not

node1.controller1.eth6	Controller 1 Eth 6	defined, these ports will be used for both data and management traffic.

Network Traffic Payload Size (Jumbo Frames)

The DVX System supports the use of jumbo frames for network traffic over the Data Node data interfaces. If you use jumbo frames, every device on the network path between the Data Node and the ESXi host must be configured for jumbo frame traffic. This includes:

- Data Node data interface.
- Switches between the Data Node and the ESXi hosts.
- VMkernel NICs on the ESXi hosts.

The DVX CLI provides the following commands to support jumbo frame payloads:

CLI Command	Description
`network jumbo-frames enable`	Enable the use of jumbo frames with a Maximum Transmission Unit (MTU) of 9000 bytes on the Data Node data interface.
`network jumbo-frames disable`	Disables the use of jumbo frames and sets the MTU to 1500 bytes.

Data Node High Availability

The DVX Data Node provides high availability through controller redundancy and network port redundancy.

- Controller Redundancy uses a pair of controllers in an active/standby configuration to provide continuous access to data.
- Network Port Redundancy uses active-active data port pairs to provide aggregate bandwidth. If there is a network path failure, the DVX System will use the remaining active port. The Data Node also supports an active/standby bonded port-pair configuration for the management interface.

- Data Node Fault Tolerance (DNFT). In DVX systems with 3 or more Data Nodes, you can activate Data Node Fault Tolerance (DNFT) to guarantee data and performance high availability for unplanned failovers due to network or power loss, maintenance operations, or disasters.

Controller Redundancy

The DVX System provides redundant Data Node controller components to support continuous access to data. The Data Node provides an active/standby HA (High Availability) capability.

The Data Node supports controller failover in response to controller failure. It also provides a dynamic controller failover capability that is based on Data Node connectivity and Compute Node connectivity.

- Controller failure – The Data Node has a pair of controllers that operate in active/standby configuration for high availability. If the active controller fails, the DVX System promotes the standby controller to active status and uses the newly active controller to continue to serve data requests.
- Data Node connectivity – With a Data Pool of more than one Data Node, a DVX System supports dynamic controller failover based on connectivity between the Data Nodes. The DVX System will failover controllers on Data Nodes to maintain connectivity between all Nodes in the Data Pool.
- Compute Node connectivity – If the following conditions are satisfied, the DVX System will failover to the standby controller.
    - The standby controller must have connectivity to more Compute Nodes than the active controller.
    - The standby controller set of Compute Nodes must include the same set of Compute Nodes that are connected to the active controller.
    - Connectivity between Data Nodes in the Data Pool is not compromised.

To support controller redundancy, you must connect cables to the ports that you will use on both controllers. When you configure the Data Node network, you identify two or more Data Node network interfaces. A single DVX network interface represents the same port on both controllers.

The following picture shows the change in data port usage if there is a controller failover. In this situation, controller 1 is the active controller. The teamed port pair eth5+eth6 is configured on the Data Node.

If controller 1 fails or if controller 2 has network connectivity to more hosts (including all the hosts with connectivity to controller 1), controller 2 becomes the active controller and the data interface on controller 2 assumes the active role. Data Node communication with ESXi hosts can continue without reconfiguration.

Floating IP Address

The Data Pool uses floating IP addresses to support the High Availability capability for controller failover. The Data Pool supports one floating IP address for the data ports and a second floating IP address for the management ports.

- The Hyperdriver on a host uses the data floating IP address to communicate with the Data Pool.
- The DVX GUI uses the management floating IP address to communicate with the Data Pool.
- Use the management floating IP address to create DVX CLI and DVX GUI connections to the Data Pool.

Regardless of any controller failover that might occur in a Data Pool, the DVX System maintains the floating IP addresses for continued access.

Network Port Redundancy

The Data Node provides adaptive path networking for data ports and bonded pair redundancy for management ports.

- Adaptive path networking uses two or more data interfaces of the same media type for aggregate bandwidth over the paired interfaces. If the network path for one of the interfaces fails, the DVX System will continue to use the bandwidth on the remaining active interface(s).

- Bonded pair management ports provide an active/passive redundant interface. If the active port fails, the passive interface becomes active and the system fails over to the newly active interface.

The following table shows the interface team possibilities for DVX traffic. You can configure only one data interface team on a Data Node. You cannot mix ports of different speeds or media types. For example, you cannot configure both eth3 and eth6 ports at the same time.

DVX Network Interface Pairs for Data and Management Traffic

Data Node Model	Traffic type	Interface Teams	Speed and Connector Type
D12x4B 2x25G D12x4C 2x25G D12x10D 2x25G F24x2B 2x25G F24x2D 2x25G	Data	eth3+eth4	2x10G BASE-T RJ45
		eth5+eth6	2x10G SFP+/25G SFP28 (optical or direct attach copper)
	Management	eth1+eth2	1G RJ45
D12x4B 4x10G	Data	eth3+eth4	10G BASE-T RJ45
		eth5+eth6	2x10G BASE-T RJ45
		eth7+eth8	2x10G BASE-T RJ45
		eth5+6+7+8	4x10G BASE-T RJ45
	Management	eth1+eth2	1G RJ45
D12x4	Data	eth5+eth6	2x10G BASE-T RJ45
		eth3+eth4	2x10G SFP+ (optical or direct attach copper)
	Management	eth1+eth2	1G RJ45

The picture below shows the change in network port usage if there is a management network failure.

- Controller 1 is the active controller.
- The eth1 and eth2 management interfaces are configured on the Data Node.
- The management ports on both controllers are bonded. Each bonded pair has a single IP address.

In this situation, the Data Node is using the eth1 port for management traffic.

- If there is a network failure, the eth2 port becomes the active management port and DVX GUI/CLI communication with the Data Node and Datrium Support operations can continue without any additional network configuration. If there is a network failover during a CLI session, you will have to log in again.
- If there is a controller failover, the management interface on controller 2 supports network failover as well.

Data Node Fault Tolerance (DNFT)

In DVX systems with 3 or more Data Nodes, you can activate Data Node Fault Tolerance (DNFT) to guarantee data and performance high availability for unplanned failovers due to network or power loss, maintenance operations, or disasters, such as when:

- An entire Data Node fails or loses power.
- A Data Node is unreachable due to power loss or network outage, or due to hardware or software failure on both controllers of a Data Node.

> **Tip:** You can also enable DNFT when adding a third Data node.

By default, DNFT is disabled. In order to activate DNFT you must have a minimum of 3 Data Nodes in your Data Pool.

Once DNFT is activated:

- One Data Node worth of storage in your Data Pool will be set aside as reserve for HA.
- Once enabled, DNFT cannot be disabled.

> **Note:** After enabling DNFT, it can take several hours before all data in the Data Pool is fully rebalanced. This process does not interfere with normal Data Pool operation.

DNFT and “Reserved” Storage

The DVX storage pool reserves storage capacity to support DNFT. This reserved space is not available for datastore file systems.

- In a DVX deployment with 2 or more Data Nodes, *without* DNFT activated, a storage pool can recover from two drive failures, because DVX always retains 2 drives worth of storage in reserve. It will use the reserve space to rebuild the contents of the failed drives.
- With DNFT activated, a DVX storage pool can recover from the amount of storage equivalent to an entire Data Node by reserving the capacity of an entire Data Node.

A Data Node’s reserve storage is measured roughly by physical storage drive capacity, but because of the way the DVX system stores and distributes data, the reserve space stored by the DVX System is not written to a physical “hot spare” drive as in a traditional RAID storage system. The disk drive measurement is only used to express the capacity of reserve storage.

Network Topology

The DVX System provides aggregate data bandwidth and continued operation in the event of a network failure.

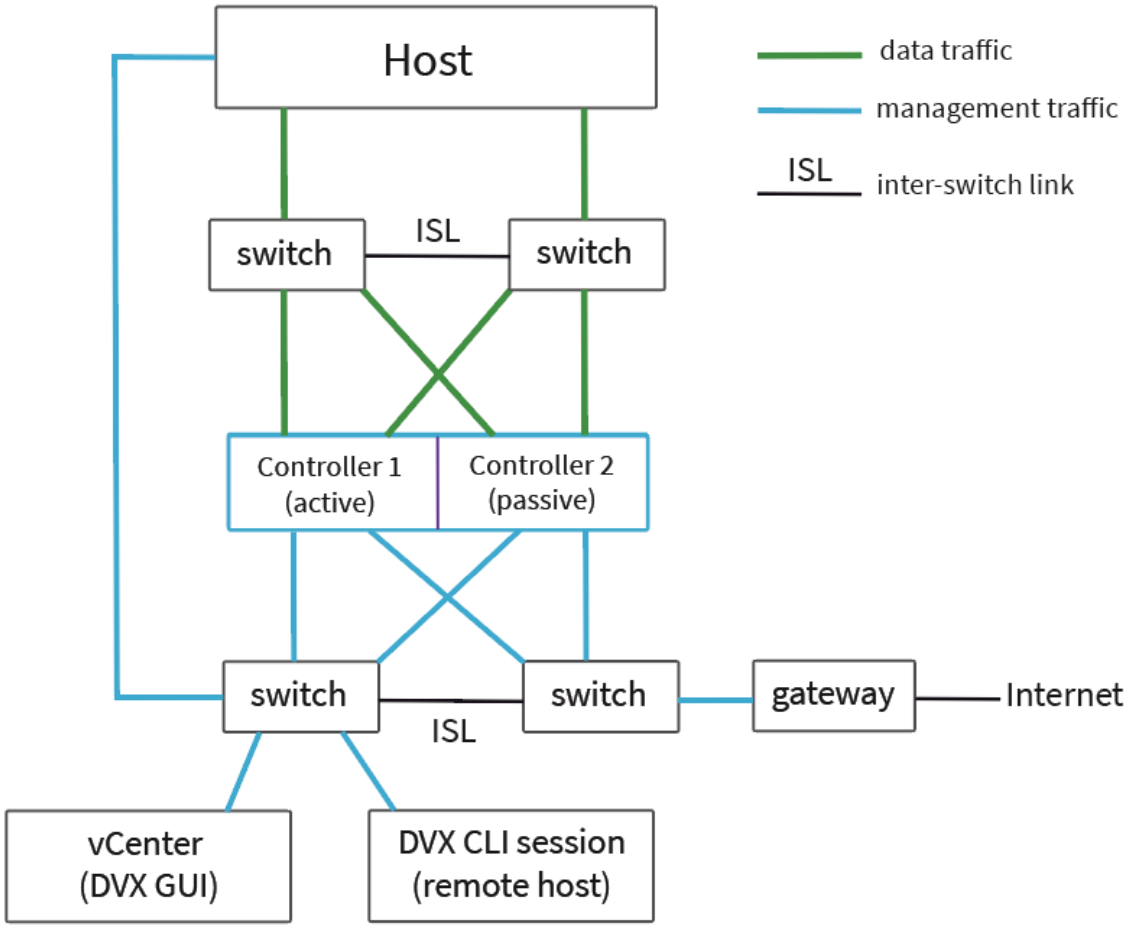
Active Data Paths

The following figure shows the data paths between hosts and the active controller on the Data Node. This topology uses the following components:

- A Data Node with teamed 10G data ports.
- Two switches that use inter-switch linking.

- Two or more hosts that use NIC teaming for the ports that will send traffic to the Data Node.

The DVX System distributes traffic across Data Node data interfaces.



- The DVX Hyperdriver on a host uses the active NIC port to send data traffic to both ports on the Data Node.
- The use of inter-switch linking supports the distribution of traffic.
- The DVX ports are teamed to support aggregate pathing. The DVX System determines active paths and uses all of the available network interfaces on the active controller.

- The DVX System supports uninterrupted data traffic in the event of a network failure along a data path. With redundant switches, the host can use the standby NIC port to send traffic to the reachable data port.

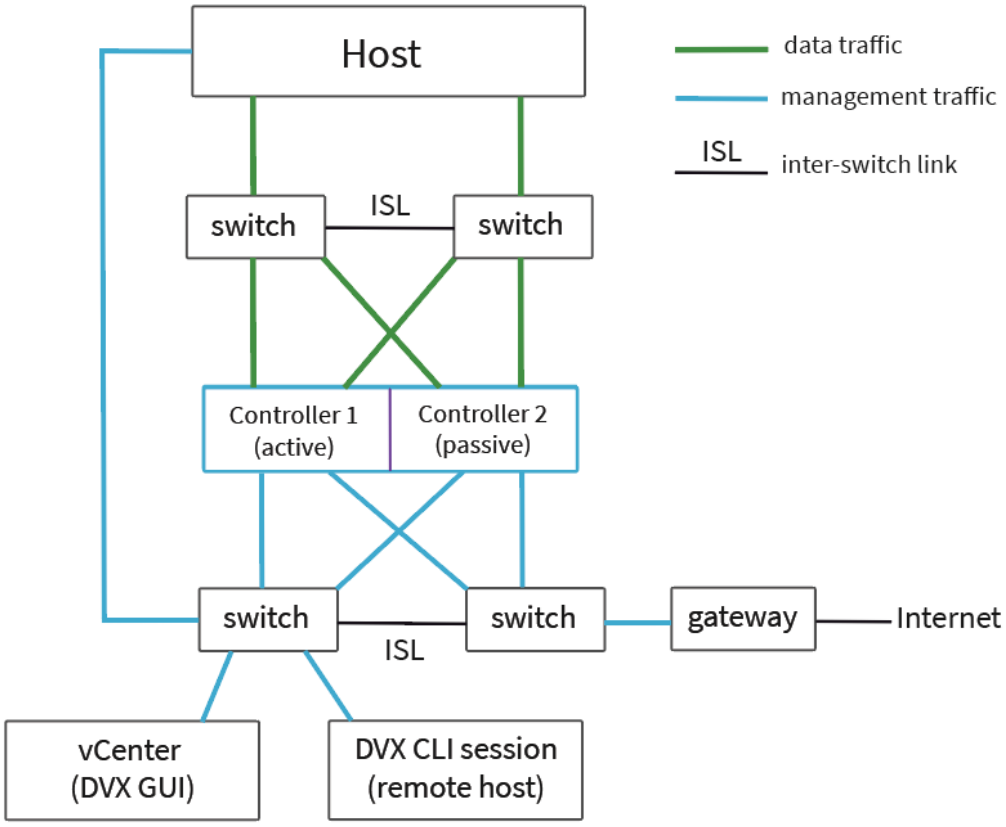
Requirements to support network failover for data traffic:

- Connect each controller's ports to multiple switches that use inter-switch linking.
- The Data Node data interfaces must be on the same subnet as the hosts.
- Use NIC teaming on the host. Use NICs that will support the desired data speed.
- Enable beacon probing on ESXi hosts.
- On Linux hosts, use the network interface active-backup bonding option.

Redundant Topology

DVX Network – High Availability shows the network topology for an environment that has separate subnets for data and management, and a Data Node that uses redundant data and management network interfaces. The gateway is on the management subnet.

DVX Network – High Availability



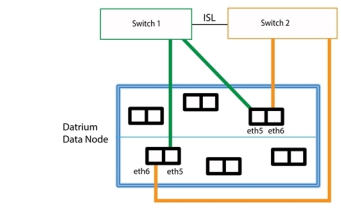
To support controller failover, there are both data and management connections to both controllers on the Data Node.

- The host uses the data subnet for communication with the Data Node.
- The host uses the management subnet for communication with the vCenter Server.
- The vCenter Server uses the management subnet for communication with the Data Node.
- UI sessions (GUI and CLI) use the management floating IP address to connect to the DVX System.

To support network failover:

- The Data Node uses teamed data interfaces and bonded management ports on both controllers.
- Switches within a subnet use inter-switch linking.
- The host uses NIC teaming for the data ports (picture below).

Network Topology – Teamed Data Ports

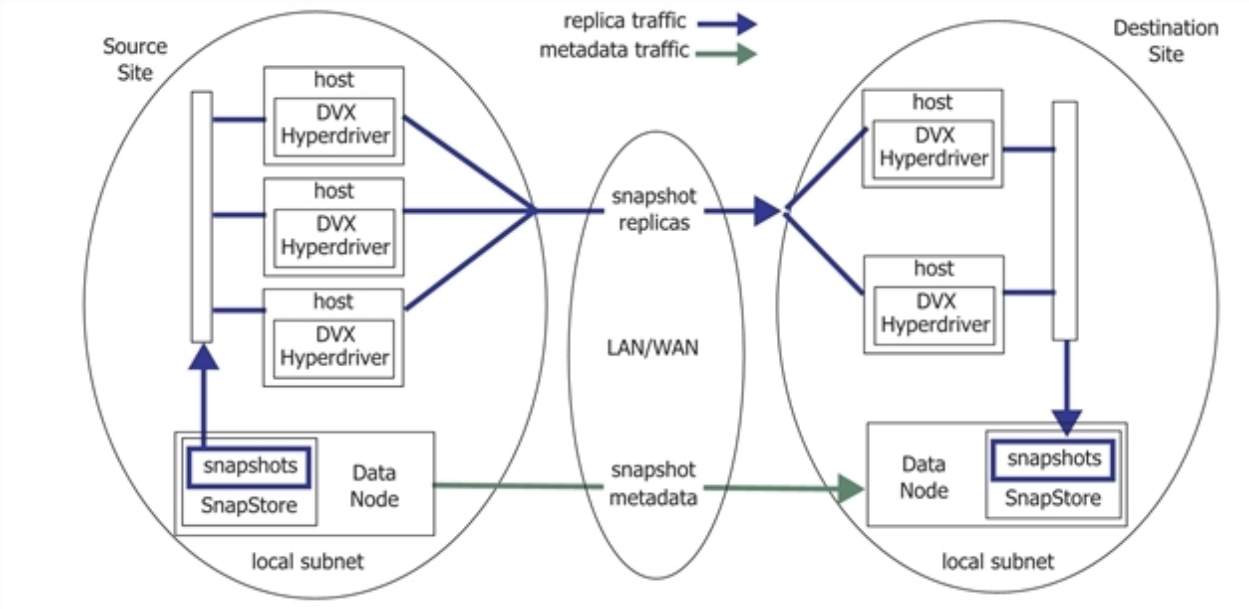


Teamed port connections:

- Connect all ports for a single interface to the same switch.
- Use inter-switch linking between switches that are connected to the Data Node.

In the picture above, both eth5 ports are connected to switch 1 and both eth6 ports are connected to switch 2. The DVX System will use both ports for data traffic. If there is a network failure on one of the ports, the other port in the team carries the load. If there is a controller failover (controller 1 fails over to controller 2), the Data Node will use the teamed ports on the second controller. If there is a network failure in one of the ports in that team, the DVX System will use the active port.

Network Support for Replication



The DVX Systems use host resources to transfer snapshot replicas.

- Each source site host must have network access to at least one IP address at each destination site host.
- Any firewalls must allow access through port 1525 for host-to-host communication.
- You can designate host ports for replication traffic.

The DVX System uses the Data Node-to-Data Node connection to transfer snapshot metadata.

- The source site Data Node must have network access to the replica site Data Node.
- Any firewalls must allow access through port 4105 for Data Node-to-Data Node communication.

If you are keeping a strict separation between data and management traffic, specify the management floating IP address when you define the replica site. (See the *DVX System Management* manual.) The DVX System uses the management interfaces for Data Node communication between the source and destination sites. The management floating IP address must be routable from all destination hosts.

Specify the management floating IP address when you define the replica site. (See the *DVX System Management* guide.) The management floating IP address must be routable from all destination hosts. The DVX System will use the management interfaces for Data Node communication between the source and destination sites.

In an individual DVX System site, source or destination, the Data Node and hosts are on the same subnet. Datrium recommends that data traffic between the host(s) and Data Node in a single DVX System should be on the same subnet.

Open Source & Third party software license notices

The page references licensing for all open source and third party software used by Datrium software.

- Source Code Offer
- Data Node (Datrium OS)
- DVX Hyperdriver
- KVM Hyperdriver
- Cloud DVX
- ControlShift Backend
- Datrium GUIs
- Additional License Notices

Source Code Offer

This software contains open source software. To the extent the license for any open source software requires VMware to make available to you the corresponding source code and/or modifications (the "Source Files"), you may obtain a copy of the applicable Source Files by sending a written request, with your name, address, and applicable VMware software product and version to: VMware, Inc., 3401 Hillview Avenue, Palo Alto, CA 94304, United States of America.

All requests should clearly specify: Open Source Files Request, Attention: General Counsel. This offer to obtain a copy of the Source Files is valid for three years from the date you acquired the VMware software.

Data Node (Datrium OS)

The following table lists the open source software used in the DVX Data Node and provides links to relevant resources.

Software	License	Link
angular-1.2.14.min.js	MIT	https://github.com/angular/angular.js/blob/master/LICENSE
angular-angular-route-1.2.14.min.js	MIT	https://github.com/angular/bower-angular-route
angular-bootstrap-datetimepicker	MIT	http://www.knightrider.com
angular-cron-jobs.js	MIT	https://github.com/jacobscarter/angular-cron-jobs
angular-date-time-input	MIT	http://www.knightrider.com
angular-animate.js	MIT	https://github.com/angular/bower-angular-animate
angular-moment.js	MIT	https://github.com/urish/angular-moment
angular-translate.js	MIT	https://github.com/angular-translate/angular-translate
Apache commons collection	Apache	http://www.apache.org/licenses/
Apache commons exec	Apache	http://www.apache.org/licenses/

Software	License	Link
Apache commons IO	Apache	http://www.apache.org/licenses/
Apache commons lang	Apache	http://www.apache.org/licenses/
Apache commons net	Apache	http://www.apache.org/licenses/
Apache commons validator	Apache	http://www.apache.org/licenses/
Apache curator	Apache	http://www.apache.org/licenses/
Apache cxf	Apache	http://www.apache.org/licenses/
Apache HTTP client	Apache	http://www.apache.org/licenses/
argparse.py	Python	Taken from Python 2.7 standard library; modified to run on ESXi Python 2.6.
Avahi 0.6.31	LPGLv2.1	https://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
AWS Java SDK	Apache License, Version 2.0	https://github.com/aws/aws-sdk-java/blob/master/LICENSE.txt
aws-java-sdk-cognitoidentity-1.11.283.jar aws-java-sdk-iam-		

Software	License	Link
1.11.142.jar aws-java-sdk-sns-1.11.283.jar aws-java-sdk-core-1.11.283.jar aws-java-sdk-kinesis-1.11.283.jar aws-java-sdk-sqs-1.11.283.jar aws-java-sdk-dynamodb-1.11.283.jar aws-java-sdk-kms-1.11.283.jar aws-lambda-java-core-1.1.0.jar aws-java-sdk-ec2-1.11.142.jar aws-java-sdk-lambda-1.11.142.jar aws-lambda-java-events-1.1.0.jar aws-java-sdk-events-1.11.142.jar aws-java-sdk-s3-1.11.283.jar aws-lambda-java-log4j-1.0.0.jar		
bash-5.0	GPLv3	https://www.gnu.org/licenses/gpl.html
bind-9.9.8-P4	ISC	https://www.isc.org/downloads/software-support-policy/isc-license/
bootstrap-3.1.1.min.js	MIT	http://bootstrapdocs.com/v3.1.1/docs/getting-started/#license-faqs
bootstrap-	Apache	https://github.com/davidstutz/bootstrap-multiselect

Software	License	Link
multiselect .css	License, Version 2.0	
bootstrap-multiselect .js	Apache License, Version 2.0	https://github.com/davidstutz/bootstrap-multiselect/blob/master/LICENSE.md
bouncycastle	MIT	https://www.bouncycastle.org/licence.html
BSD qsort	3-clause BSD	http://opensource.org/licenses/BSD-3-Clause
busybox-1.21.0	GPLv2	http://www.busybox.net/license.html
bzip2-1.0.6	Linux SPDX	https://spdx.org/licenses/bzip2-1.0.6.html
cppunit-1.12.1	LPGLv2.1	http://www.gnu.org/copyleft/lesser.html
CityHash	MIT	https://github.com/nashby/cityhash/blob/master/LICENSE.txt
commons-codec-1.6.jar	Apache License, Version 2.0	http://www.apache.org/licenses/
commons-lang3-3.2.jar	Apache License, Version 2.0	http://www.apache.org/licenses/
commons-logging-1.1.3.jar	Apache License, Version 2.0	http://commons.apache.org/proper/commons-logging/
commons-net-3.2.jar	Apache License, Version 2.0	http://www.apache.org/licenses/
cookielib.py	Python	http://svn.python.org/projects/python/branches/release27-maint/Lib/cookielib.py

Software	License	Link
coreutils-8.21	GPLv3	https://www.gnu.org/licenses/gpl.html
corkscrew-2.0	GPLv2	https://www.gnu.org/licenses/old-licenses/gpl-2.0.html
crash-7.2.5	GPLv3	https://github.com/crash-utility/crash/blob/master/COPYING3
CRC	Apache License, Version 2.0	http://www.apache.org/licenses/LICENSE-2.0
d3.min.js	BSD	http://d3js.org/
dbus-1.10.14	GPLv2	https://www.gnu.org/licenses/old-licenses/gpl-2.0.html
dialog-1.2-20150225	LPGLv2.1	https://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
dmidecode-2.11	GPLv2	https://www.gnu.org/licenses/old-licenses/gpl-2.0.html
dstat 0.7.2-7.fc17	GPLv2	https://www.gnu.org/licenses/old-licenses/gpl-2.0.html
dropbear-2012.55	dropbear license	https://secure.ucc.asn.au/hg/dropbear/file/57d09741d46d/LICENSE
e2fsprogs-1.42.7	GPLv2	https://www.gnu.org/licenses/old-licenses/gpl-2.0.html
	MIT	https://github.com/stephenc/eaio-uuid/blob/master/copying.txt
elfutils-0.174	LGPLv3	https://www.gnu.org/licenses/lgpl-3.0.en.html
ethtool-4.8	GPLv2	http://git.kernel.org/cgit/network/ethtool/ethtool.git/tree/COPYING

Software	License	Link
exp4j	Apache	https://github.com/fasseg/exp4j/blob/master/LICENSE
expat-2.0.1	MIT	https://opensource.org/licenses/MIT
file-5.32	custom	https://github.com/file/file/blob/d474e35513940dbca039b510b4de705b44f5bd9c/COPYING
fileLeakDetector	MIT	https://github.com/kohsuke/file-leak-detector/blob/master/LICENSE.txt
fping-3.13	custom	https://github.com/schweikert/fping/blob/18df5bc5394f8cc42f60469b08ee600d58480d89/src/fping.c#L20
font-awesome-4.3.0	SIL OFL 1.1	https://fortawesome.github.io/Font-Awesome/license/
font-awesome.min.css	MIT (Code License)	https://fortawesome.github.io/Font-Awesome/license/
gdb-7.6	GPLv3	https://www.gnu.org/licenses/gpl.html
glib-2.36.0	LGPLv2	https://www.gnu.org/licenses/old-licenses/lgpl-2.0.html
glibc-2.12.2	LGPLv2.1	https://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
glob2	Python	http://code.activestate.com/recipes/578078/
google protobuf	BSD	https://github.com/google/protobuf/blob/master/LICENSE
gptfdisk-0.8.7	GPLv2	https://www.gnu.org/licenses/old-licenses/gpl-2.0.html
greenmail	Apache	https://github.com/greenmail-mail-test/greenmail/blob/master/license.txt
grub 0.97	GPLv3	https://www.gnu.org/licenses/gpl.html

Software	License	Link
guava	Apache	https://github.com/google/guava/blob/master/COPYING
guava-18.0.jar	Apache License, Version 2.0	https://code.google.com/p/guava-libraries/
gzip-1.5	GPLv3	https://www.gnu.org/licenses/gpl.html
httpclient-4.3.1.jar	Apache License, Version 2.0	https://hc.apache.org/downloads.cgi
httpcore-4.3.jar	Apache License, Version 2.0	https://code.google.com/p/guava-libraries/
ini4j	Apache	http://www.apache.org/licenses/
Intel ISA-L_crypto	Intel	https://github.com/01org/isa-l_crypto
iperf-2.0.5	BSD-2-Clause	https://opensource.org/licenses/BSD-2-Clause
ipmitool-1.8.12	ipmitool license	http://ipmitool.cvs.sourceforge.net/viewvc/ipmitool/ipmitool/COPYING?revision=1.2&view=markup
iproute2-3.6.0	GPLv2	https://www.gnu.org/licenses/old-licenses/gpl-2.0.html
iptables 1.6.1	GPLv2	https://www.gnu.org/licenses/old-licenses/gpl-2.0.html
iputils-s20121125	GPLv2	https://www.gnu.org/licenses/old-licenses/gpl-2.0.html
irqbalance 1.1.0	GPLv2	https://www.gnu.org/licenses/old-licenses/gpl-2.0.html
irqstat	MIT	https://opensource.org/licenses/MIT

Software	License	Link
902c7b5		
isa-l 2.21.0	BSD-3-Clause	https://opensource.org/licenses/BSD-3-Clause
isa-l_crypto 2.16	BSD-3-Clause	https://opensource.org/licenses/BSD-3-Clause
jackson	Apache	http://www.apache.org/licenses/
jackson-annotations-2.4.0.jar	Apache License, Version 2.0	http://www.apache.org/licenses/LICENSE-2.0
jackson-databind-2.4.0.jar	Apache License, Version 2.0	https://code.google.com/p/guava-libraries/
jacoco	Eclipse	http://eclemma.org/license.html
jansson-2.9	MIT	https://opensource.org/licenses/MIT
java-1.8.0-openjdk-1.8.0.45-28.b13.el6_6.x86_64		
javamail	CDDL & GPLv2 w/ classpath exception	https://java.net/projects/javamail/pages/License
jcommander	Apache	http://www.apache.org/licenses/
Jerasure	BSD 3-Clause	https://github.com/tsuraan/Jerasure/blob/master/License.txt
jeromq	LGPL	https://github.com/zeromq/jeromq/blob/master/COPYING.LESSER

Software	License	Link
jetty	Dual license under Apache & eclipse	http://www.eclipse.org/jetty/licenses.php
jna	Dual license under Apache & LGPL	https://github.com/java-native-access/jna/blob/master/LICENSE
jquery-2.1.0.min.js	MIT	https://jquery.org/license/
jquery.class.js	MIT	https://github.com/mach3/js-jquery-class
jquery.qtip.min.js	MIT/GPLv2	http://qtip2.com/
jsonpath	Apache	http://www.apache.org/licenses/
kexec-tools-2.0.7	GPLv2	https://www.gnu.org/licenses/old-licenses/gpl-2.0.html
kmod 24	LGPLv2.1	https://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
libaio 0.3.109	LGPLv2.1	https://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
libarchive 3.3.1	BSD-3-Clause	https://raw.githubusercontent.com/libarchive/libarchive/master/COPYING
libcurl	MIT	https://curl.haxx.se/docs/copyright.html
libdaemon 0.14	LGPLv2.1	https://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
libffi 3.0.13	MIT	https://opensource.org/licenses/MIT
libmnl	LGPLv2.1	https://www.gnu.org/licenses/old-licenses/lgpl-2.1.html

Software	License	Link
1.0.4		
libnftnl 1.0.7	GPLv2	https://www.gnu.org/licenses/old-licenses/gpl-2.0.html
libpcap 1.8.1	BSD-3-Clause	https://opensource.org/licenses/BSD-3-Clause
libtirpc 1.0.1	BSD-3-Clause	https://opensource.org/licenses/BSD-3-Clause
libumberlog	BSD	https://raw.githubusercontent.com/deirf/libumberlog/master/LICENSE
linux-3.10.0-123.el7	GPLv2	https://www.kernel.org/pub/linux/kernel/COPYING
Linux-PAM 1.2.1	GPL+BSD-3-Clause	https://github.com/linux-pam/linux-pam/blob/e89d4c97385ff8180e6e81e84c5aa745daf28a79/COPYING
lm_sensors-3.3.2	GPLv2	https://www.gnu.org/licenses/old-licenses/gpl-2.0.html
log4j-1.2.17.jar	Apache License, Version 2.0	https://logging.apache.org/log4j/1.2/download.html
_LWPCookieJar.py	Python	http://svn.python.org/projects/python/trunk/Lib/_LWPCookieJar.py
lz4-1.8.3	BSD 2-Clause and GPLv2	https://github.com/lz4/lz4/blob/dev/LICENSE
makedumpfile-1.5.7	GPLv2	https://www.gnu.org/licenses/old-licenses/gpl-2.0.html

Software	License	Link
mcelog 135	GPLv2	https://www.gnu.org/licenses/old-licenses/gpl-2.0.html
mDNSResponder-320-18	Apple	http://www.opensource.apple.com/source/mDNSResponder/mDNSResponder-320.10/LICENSE
mft 4.11.0-103	GPLv2+BSD-2-Clause	https://github.com/Mellanox/mstflint/blob/b5067fb45732928b63ae66ca567a39575faf1c13/LICENSE
moment.js	MIT	http://momentjs.com/
moment-timezone.js version 0.5.10	MIT	http://github.com/moment/moment-timezone
MozillaCookieJar.py	Python	http://svn.python.org/projects/stackless/Python-2.4.2/orig/Lib/_MozillaCookieJar.py
nanopb	zlib license	https://github.com/nanopb/nanopb
ncurses 5.9	custom (MIT-like)	https://github.com/gittup/ncurses
ncurses 6.0-20170325	custom (MIT-like)	https://github.com/gittup/ncurses
netcat-0.7.1	GPLv2	https://directory.fsf.org/wiki/License:GPL-2.0-or-later
net-tools-2.0.20121106	GPLv2	https://www.gnu.org/licenses/old-licenses/gpl-2.0.html
ngStorage-0.3.0.min.js	MIT	https://github.com/gsklee/ngStorage/blob/master/LICENSE
nss 3.27.1	GPLv2+MPL2.0+LGPLv2	https://github.com/nss-dev/nss/blob/master/COPYING

Software	License	Link
nss-mdns 0.10	LGPLv2.1	https://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
ntp-4.2.8p12	NTP	https://opensource.org/licenses/NTP
open-vm-tools-9.4.0-1280544	LGPLv2.1	https://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
OpenJDK 1.8.0.45-28.b13	GPLv2 +Linking Exception	http://openjdk.java.net/legal/gplv2+ce.html
openssh-7.9p1	Custom	https://github.com/openssh/openssh-portable/blob/d38f05dbdd291212bc95ea80648b72b7177e9f4e/LICENCE
OpenSSL 0.9.8y OpenSSL 2.0.12-fips	OpenSSL	https://www.openssl.org/source/license.html
patchelf-0.9	Debian/SPI	https://www.debian.org/license
pciutils-3.2.1	GPLv2	https://www.gnu.org/licenses/old-licenses/gpl-2.0.html
pkg-config-0.27	Creative Commons	https://creativecommons.org/licenses/by/3.0/
pigz 2.3.4	Zlib	https://opensource.org/licenses/Zlib
popt 1.13	X Consoritum/ MIT	https://www.x.org/releases/X11R7.7/doc/xorg-docs/License.html
procps-	GPLv2	https://www.gnu.org/licenses/old-licenses/gpl-2.0.html

Software	License	Link
3.2.8		
protobuf-3.0.0	Google	https://github.com/protocolbuffers/protobuf/blob/master/LICENSE
python 2.7.12	Python-2.0	https://opensource.org/licenses/Python-2.0
Quartz Scheduler	Apache 2.0	http://www.quartz-scheduler.org/overview/license.html
readline 6.2	GPLv3	https://www.gnu.org/licenses/gpl.html
requests	Apache 2.0	http://python-requests.org
screen 4.5.1	GPLv3	https://www.gnu.org/licenses/gpl.html
seachest-lite-1.0.1-1_18_3	Seagate	https://github.com/Seagate/ToolBin/blob/master/SeaChest/ReadMeFirst.SeaChest.txt
sg3_utils-1.34	various	https://github.com/hreinecke/sg3_utils/blob/89b09a7d159277646410d7f0f4c11a1669d931e3/COPYING
slf4j	MIT	http://www.slf4j.org/license.html
slf4j-api-1.7.2.jar	X11 License	http://www.slf4j.org/license.html
slf4j-log4j12-1.7.2.jar	X11 License	http://www.slf4j.org/license.html
smartmontools-7.0	GPLv2	https://www.gnu.org/licenses/old-licenses/gpl-2.0.html
Snappy	Like BSD:	https://github.com/google/snappy/blob/master/COPYING

Software	License	Link
	Free and open source software: Snappy is licensed under a BSD-type license.	
spring	Apache	http://www.apache.org/licenses/
spring-aop-3.2.1.RELEASE.jar	Apache License, Version 2.0	https://github.com/spring-projects/spring-framework
spring-beans-3.2.1.RELEASE.jar	Apache License, Version 2.0	https://github.com/spring-projects/spring-framework
spring-context-3.2.1.RELEASE.jar	Apache License, Version 2.0	https://github.com/spring-projects/spring-framework
spring-core-3.2.1.RELEASE.jar	Apache License, Version 2.0	https://github.com/spring-projects/spring-framework
spring-expression-3.2.1.RELEASE.jar	Apache License, Version 2.0	https://github.com/spring-projects/spring-framework
sshpass-1.06	GPLv2	https://www.gnu.org/licenses/old-licenses/gpl-2.0.html

Software	License	Link
strace-4.7	BSD3-Clause	https://opensource.org/licenses/BSD-3-Clause
stress-1.0.4	GPLv2	https://www.gnu.org/licenses/old-licenses/gpl-2.0.html
sysstat-10.0.5	GPLv2	https://www.gnu.org/licenses/old-licenses/gpl-2.0.html
tcpdump 4.9.0	BSD 3-Clause	https://opensource.org/licenses/BSD-3-Clause
testng	Apache	http://www.apache.org/licenses/
traceroute-2.1.0	GPLv2	https://www.gnu.org/licenses/old-licenses/gpl-2.0.html
tzdata 2016j	various	https://github.com/eggert/tz/blob/master/LICENSE
ui-bootstrap-tpls-0.11.2.min.js	MIT	https://angular-ui.github.io/bootstrap/
ui-grid.3.0.0-rc.21.min	MIT	https://github.com/angular-ui/bower-ui-grid
ui-grid.3.0.0-rc.21.min.css	MIT	https://github.com/angular-ui/bower-ui-grid
ui-grid.3.0.7-rc.21.min	MIT	https://github.com/angular-ui/bower-ui-grid
ui-grid.3.0.7-	MIT	https://github.com/angular-ui/bower-ui-grid

Software	License	Link
rc.21.min.css		
unzip 6.0	Info-ZIP	https://github.com/LuaDist/unzip/blob/master/LICENSE
util-linux 2.22.2	GPLv2	https://www.gnu.org/licenses/old-licenses/gpl-2.0.html
uuid 1.6.2	MIT	https://opensource.org/licenses/MIT
Xyratex USM	Altera	https://www.altera.com/support/support-resources/download/licensing/lic-jam.html
	Apache 2.0	http://www.apache.org/licenses/LICENSE-2.0
	BSD 2-Clause	https://opensource.org/licenses/BSD-2-Clause
	BSD 3-Clause	http://opensource.org/licenses/BSD-3-Clause
	Bzip2	Bzip2 License
	Eclipse Public License	https://www.eclipse.org/legal/epl-v10.html
	GPL v2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
	MIT	https://fedoraproject.org/wiki/Licensing:MIT?rd=Licensing/MIT
	OpenLDAP	http://www.openldap.org/software/release/license.html
	OpenSSL	http://www.sdisw.com/openssl.htm
	Original SSLeay	Original SSLeay License
	Vprintf	vprintf License
zip 3.0	Info-ZIP	http://infozip.sourceforge.net/license.html

Software	License	Link
zlib 1.2.7	Zlib	https://opensource.org/licenses/Zlib
zookeeper-c 3.5.5	Apache-2.0	http://www.apache.org/licenses/LICENSE-2.0

Additional License Notices

- Intel License
- platform.py
- ptmalloc3
- Original SSLeay License
- vprintf License

Intel License

Copyright(c) 2011-2016 Intel Corporation All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Intel Corporation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE

LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

platform.py

Copyright (c) 1999-2000, Marc-Andre Lemburg; mailto:mal@lemburg.com
Copyright (c) 2000-2003, eGenix.com Software GmbH; mailto:info@egenix.com

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee or royalty is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation or portions thereof, including modifications, that you make.

EGENIX.COM SOFTWARE GMBH DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE !

ptmalloc3

Copyright (c) 2001-2006 Wolfram Gloger

Permission to use, copy, modify, distribute, and sell this software and its documentation for any purpose is hereby granted without fee, provided that (i) the above copyright notices and this permission notice appear in all copies of the software and related documentation, and (ii) the name of Wolfram Gloger may not be used in any advertising or publicity relating to the software.

THE SOFTWARE IS PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EXPRESS, IMPLIED OR OTHERWISE, INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

IN NO EVENT SHALL WOLFRAM GLOGER BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES OF ANY KIND, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER OR NOT ADVISED OF THE POSSIBILITY OF DAMAGE, AND ON ANY THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

ptmalloc3 uses malloc, which contains the following statement:

This is a version (aka dlmalloc) of malloc/free/realloc written by Doug Lea and released to the public domain, as explained at http://creativecommons.org/licenses/publicdomain. Send questions, comments, complaints, performance data, etc to dl@cs.oswego.edu.

Original SSLeay License

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).The implementation was written so as to conform with Netscapes SSL.This library is free for commercial and non-commercial use as long asthe following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

vprintf License

Copyright (c) 1990 The Regents of the University of California. All rights reserved.

This code is derived from software contributed to Berkeley by Chris Torek.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

DVX Hyperdriver

Software	License	Link
cppunit-1.12.1	LGPLv2.1	https://www.gnu.org/copyleft/lesser.html
curl-7.57	Curl	https://curl.haxx.se/docs/copyright.html
isa-l-crypto-2.16	BSD-3-Clause	https://github.com/01org/isa-l_crypto/blob/master/LICENSE
elfutils-0.174	LGPLv3	https://www.gnu.org/licenses/lgpl-3.0.en.html

Software	License	Link
eaio-uuid	MIT	https://github.com/stephenc/eaio-uuid/blob/master/copying.txt
jansson-2.9	MIT	https://opensource.org/licenses/mit-license.php
libarchive-3.3.1	BSD-3 Clause	https://raw.githubusercontent.com/libarchive/libarchive/master/COPYING
nvdk-5.5.0	VMware	https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/universal_eula.pdf
openssl-fips-2.0.12	OpenSSL/SSLeay	https://www.openssl.org/source/license.html
patchelf-0.9	Debian/SPI	https://www.debian.org/license
protobuf-3.0.0	Google	https://github.com/protocolbuffers/protobuf/blob/master/LICENSE
python 2.7.12	Python-2.0	https://opensource.org/licenses/Python-2.0
vibtools-5.5.0	VMware	https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/universal_eula.pdf
zlib 1.2.7	Zlib	https://opensource.org/licenses/Zlib
zookeeper-c 3.4.6	Apache-2.0	http://www.apache.org/licenses/LICENSE-2.0

KVM Hyperdriver

Software	License	Link
glibc-2.12.2	LGPLv2.1	https://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
python 2.7.12	Python-2.0	https://opensource.org/licenses/Python-2.0

Cloud DVX

Software	License	Link
libxml2-2.9.1	MIT	https://opensource.org/licenses/mit-license.html
lxml-4.2.1	BSD-3-Clause	https://lxml.de/index.html#license
openssl-1.0.2c	Apache-2.0	https://www.openssl.org/source/license.html
openssl-1.0.2h-fips	Apache-2.0	https://www.openssl.org/source/license.html
pyopenssl	Apache-2.0	https://github.com/pyca/pyopenssl/blob/master/LICENSE
vsphere-automation-sdk-python	MIT	https://github.com/vmware/vsphere-automation-sdk-python/blob/master/LICENSE

ControlShift Backend

Software	License	Link
aws-java-sdk-ses:1.11.378	Amazon	https://github.com/aws/aws-sdk-java/blob/master/LICENSE.txt

Software	License	Link
boto3 1.5.12	Amazon	https://github.com/boto/boto3/blob/develop/LICENSE
Golang 1.9.2	Go Authors	https://github.com/golang/go/blob/master/LICENSE
googleapis-common-protos:0.0.3	Google21	https://github.com/googleapis/api-common-protos/blob/master/LICENSE
io.grpc:grpc-netty:1.9.0	Apache 2.0	https://github.com/grpc/grpc-java/blob/master/LICENSE
io.grpc:grpc-protobuf:1.9.0	Apache 2.0	https://github.com/grpc/grpc-java/blob/master/LICENSE
io.grpc:grpc-stub:1.9.0	Apache 2.0	https://github.com/grpc/grpc-java/blob/master/LICENSE
io.grpc:grpc-testing:1.9.0	Apache 2.0	https://github.com/grpc/grpc-java/blob/master/LICENSE
opentable/otj-pg-embedded	Apache 2.0	https://github.com/opentable/otj-pg-embedded/blob/master/LICENSE.txt
pgcli 2.1.0	BSD-3 Clause	https://github.com/dbcli/pgcli/blob/master/LICENSE.txt
postgresql:42.2.1.jre7	Open Source Initiative	https://opensource.org/licenses/PostgreSQL
protobuf-java-util:3.5.1	Google	https://github.com/protocolbuffers/protobuf/blob/master/LICENSE
reged 0.1 140201	LGPLv2.1	https://github.com/rescatux/chntpw/blob/master/LGPL.txt
zstd-1.4.4	BSD-3 Clause	https://github.com/facebook/zstd/blob/dev/LICENSE

Datrium GUIs

This section lists the open source software used in the DVX and ControlShift GUIs and provides links to relevant resources.

DVX GUI

Software	License	Link
browserify 14.4.0	MIT	https://github.com/browserify/browserify/blob/master/LICENSE
browserify-compile-templates 0.1.3	None	None
browserify-transform-tools 1.2.2	MIT	https://github.com/benbria/browserify-transform-tools/blob/master/LICENSE
coffee-script 1.8.0	MIT	https://github.com/jashkenas/coffeescript/blob/master/LICENSE
coffeeify	MIT	https://spdx.org/licenses/MIT
convert-source-map 0.4.1	MIT	https://github.com/thlorenz/convert-source-map/blob/master/LICENSE
core-util-is 1.0.1	MIT	https://github.com/isaacs/core-util-is/blob/master/LICENSE
domelementtype 1.1.3	BSD 2-Clause	https://github.com/fb55/domelementtype/blob/master/LICENSE
domhandler 2.2.1	BSD 2-Clause	https://github.com/fb55/domhandler/blob/master/LICENSE
domutils	BSD 2-	https://github.com/fb55/domutils/blob/master/LICENSE

Software	License	Link
1.5.0	Clause	
entities 1.0.0	BSD 2-Clause	https://github.com/fb55/entities/blob/master/LICENSE
esprima 4.0.0	BSD 2-Clause	https://github.com/jquery/esprima/blob/master/LICENSE.BSD
falafel 0.3.1	MIT	https://spdx.org/licenses/MIT
fs 0.0.1-security	ISC	https://opensource.org/licenses/ISC
htmlparser2 3.7.3	MIT	https://static.fsf.org/nosvn/directory/fdl-1.3-standalone.html
inherits 2.0.1	ISC	https://opensource.org/licenses/ISC
isarray 0.0.1	MIT	https://github.com/juliangruber/isarray
jasmine-core 2.8.0	MIT	https://github.com/jasmine/jasmine/blob/master/MIT.LICENSE
jshint	MIT	https://github.com/jshint/jshint/blob/master/LICENSE
karma 1.7.1	MIT	https://github.com/karma-runner/karma/blob/master/LICENSE
karma-chrome-launcher 2.2.0	MIT	https://github.com/karma-runner/karma-chrome-launcher/blob/master/LICENSE
karma-jasmine 1.1.0	MIT	https://github.com/karma-runner/karma-jasmine/blob/master/LICENSE
karma-spec-reporter 0.0.31	MIT	https://github.com/mlex/karma-spec-reporter/blob/master/LICENSE
less 2.7.2	Apach	https://github.com/less/less.js/blob/master/LICENSE

Software	License	Link
	e-2.0	
mkdirp 0.3.5	MIT	https://www.cognigram.us/cognigram/assets/media/documents/licenses/client-npm/mkdirp-0.3.5.html
path 0.12.7	MIT	https://github.com/jinder/path/blob/master/LICENSE
puppeteer 0.10.2	Apache-2.0	https://github.com/GoogleChrome/puppeteer/blob/master/LICENSE
readable-stream 1.1.13	Node.js	https://github.com/nodejs/readable-stream/blob/master/LICENSE
replace 0.3.0	MIT	https://spdx.org/licenses/MIT
semver 4.2.0	Creative Commons	https://creativecommons.org/licenses/by/3.0/
string_decoder 0.10.31	MIT	https://www.cognigram.us/cognigram/assets/media/documents/licenses/cbbreport-npm/string_decoder-0.10.31.html
strip-comment 1.1.3	ISC	https://opensource.org/licenses/ISC
through 2.3.6	MIT	https://github.com/dominictarr/through/blob/master/LICENSE.MIT
uglify-js 3.1.2	BSD-2-Clause	https://github.com/mishoo/UglifyJS2/blob/master/LICENSE
underscore 1.7.0	MIT	https://github.com/jashkenas/underscore/blob/master/LICENSE

ControlShift GUI

Software	License	Link
big-integer1.6.32	Unlicense	https://unlicense.org/
can-ndjson-stream 1.0.2	MIT	https://github.com/canjs/can-ndjson-stream
core-js 3.6.5	MIT	https://github.com/zloirock/core-js
d3 4.13.0	BSD-3-Clause	https://github.com/d3/d3/blob/master/LICENSE
dompurify 1.0.10	Apache-2.0	https://github.com/cure53/DOMPurify/blob/master/LICENSE
google-protobuf 3.6.0	Google	https://github.com/protocolbuffers/protobuf/blob/master/LICENSE
mdn-polyfills 5.20.0	MIT	https://github.com/msn0/mdn-polyfills
moment 2.22.2	MIT	https://github.com/moment/moment/blob/develop/LICENSE
moment-timezone 0.5.31	MIT	https://github.com/moment/moment-timezone
protobufjs 6.8.6	BSD-3-Clause	https://github.com/dcodeIO/protobuf.js/blob/master/LICENSE
q 1.5.1	MIT	https://github.com/kriskowal/q/blob/master/LICENSE
re-reselect 2.1.0	MIT	https://github.com/toomuchdesign/re-reselect

Software	License	Link
react 16.4.1	MIT	https://github.com/facebook/react/blob/master/LICENSE
react-beautiful-dnd 7.1.3	Apache-2.0	https://github.com/atlassian/react-beautiful-dnd/blob/master/LICENSE
react-bootstrap 0.32.1	MIT	https://github.com/react-bootstrap/react-bootstrap/blob/master/LICENSE
react-data-grid 3.0.11	MIT	https://github.com/adazzle/react-data-grid/blob/master/LICENSE
react-dom 16.4.1	MIT	https://github.com/facebook/react/blob/master/LICENSE
react-draggable 3.3.2	MIT	https://github.com/STRML/react-draggable
react-ellipsis-with-tooltip 1.0.8	MIT	https://github.com/amirfefer/react-ellipsis-with-tooltip/blob/master/LICENSE
react-intl 2.4.0	Yahoo	https://github.com/yahoo/react-intl/blob/master/LICENSE.md
react-modal 3.0.0	MIT	https://github.com/reactjs/react-modal/blob/master/LICENSE
react-moment 0.7.9	MIT	https://github.com/headzoo/react-moment/blob/master/LICENSE
react-redux 5.0.7	MIT	https://github.com/reduxjs/react-redux/blob/master/LICENSE.md
react-router	MIT	https://github.com/ReactTraining/react-router

Software	License	Link
4.3.1		
react-router-dom 4.2.2	MIT	https://github.com/ReactTraining/react-router/blob/master/LICENSE
react-scripts 1.1.4	MIT	https://github.com/facebook/create-react-app/blob/master/LICENSE
react-virtualized 9.20.1	MIT	https://github.com/bvaughn/react-virtualized
redux 3.7.2	MIT	https://github.com/reduxjs/redux/blob/master/LICENSE.md
redux-logger 3.0.6	MIT	https://github.com/LogRocket/redux-logger/blob/master/LICENSE
redux-thunk 2.3.0	MIT	https://github.com/reduxjs/redux-thunk
reselect	MIT	https://github.com/reduxjs/reselect/blob/master/LICENSE

Additional License Notices

The following table lists additional software used in the DVX System.

Software	License
Highsoft	Highsoft OEM license
Paragon	Paragon OEM license