
Perform Manual Hardening for Versa Director

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

This article describes the Versa recommended manual hardening for Versa Director Releases 20.2 and later. System hardening ensures that Versa products are secure when running in customer networks.

Use Signed SSL Certificates

By default, Director nodes work with autogenerated, self-signed certificates. Production equipment must have a valid signed certificate so that devices accessing the infrastructure do not trigger certificate errors.

To enable secure mode, you must have installed all Versa Director and Analytics devices with production certificates and verified their functionality.

Note: Enabling secure mode has consequences for the procedures described in this article. It is advisable that you verify the working condition of all system functions before you enable secure mode.

To enable SSL certificates:

1. Generate a certificate signing request (CSR) by running the vnms-csrgen.sh script. For example:

```
$ su - versa
$ cd /opt/versa/vnms/scripts
$ sudo -u versa /opt/versa/vnms/scripts/vnms-csrgen.sh --domain director1 --country US
--state CA --locality SC --organization versa-networks.com --organizationalunit IT
--email admin@versa-networks.com --keypass versa123 --validity 365 --san director1,DNS:10.48.61.
10
```

2. Verify that the key and CSR have been created.

```
$ ls /var/versa/vnms/data/certs/domain.*
```

3. Copy the certificate to the Certificate Authority (CA) and sign it. Note the following:
 - The CSR must be in the /var/versa/vnms/data/certs/ directory.
 - The certificate must be signed with the subjective alternate names for both the active and standby Director nodes and both their IP addresses.
 - The signed certificate must be in PEM file format.
4. After you have the signed certificate, log in to the Director node.

```
| admin@director1:~$ sudo su - versa
```

5. In the versa user's home directory, create a temporary directory for the signed certificate, private key, and CA certificate, and assign the directory 700 permission:

```
| versa@director1:~$ mkdir certs  
versa@director1:~$ chmod 700 certs
```

6. Copy the signed certificate, private key, and CA certificate to the cert directory.
7. Change to the /opt/versa/vnms/scripts directory:

```
| versa@director1:~$ cd /opt/versa/vnms/scripts/
```

8. Install the SSL certificate. Note that the private key is stored in the /var/versa/vnms/data/certs/certificate-name.key file.

```
| versa@director1:/opt/versa/vnms/scripts$ ./vnms-import-key-cert.sh \  
--storepass versa123 \  
--key /home/versa/certs/director1.key \  
--cert /home/versa/certs/director1.cer.pem \  
--keypass versa123 \  
--cafile /home/versa/certs/ca.cer.pem
```

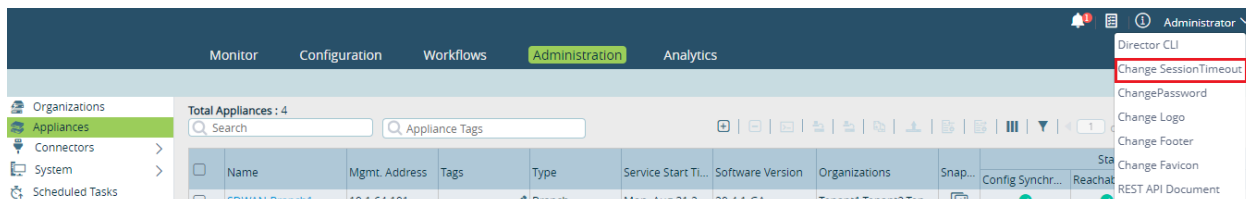
9. Copy the certificate and private key files to the standby Director node, and repeat Steps 4 through 8.
10. Securely back up and store the certificate and private key files generated in Steps 2 and 3 to a secure location using the scp command.
11. Delete the certificate and private key files generated in Steps 2 and 3 so that the private key is not left for anyone to read.

Modify the Director GUI Session Timeout

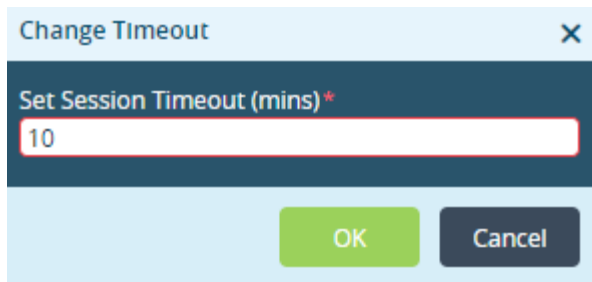
By default, the Director GUI timeout is set to 15 minutes. You can choose to decrease this time to increase Director security.

To modify the Director GUI session timeout value:

1. Log in to the Director GUI as the user Administrator.
2. In the Administrator user drop-down, select Change Session Timeout.



3. Set the desired value for the Director GUI timeout, in minutes.

A screenshot of a 'Change Timeout' dialog box. The dialog has a title bar with 'Change Timeout' and a close button (X). Below the title bar is a dark blue header with the text 'Set Session Timeout (mins) *'. Underneath is a text input field containing the number '10'. At the bottom of the dialog are two buttons: a green 'OK' button and a dark blue 'Cancel' button.

4. Click OK.
5. Repeat Steps 1 through 4 for the Operator user.

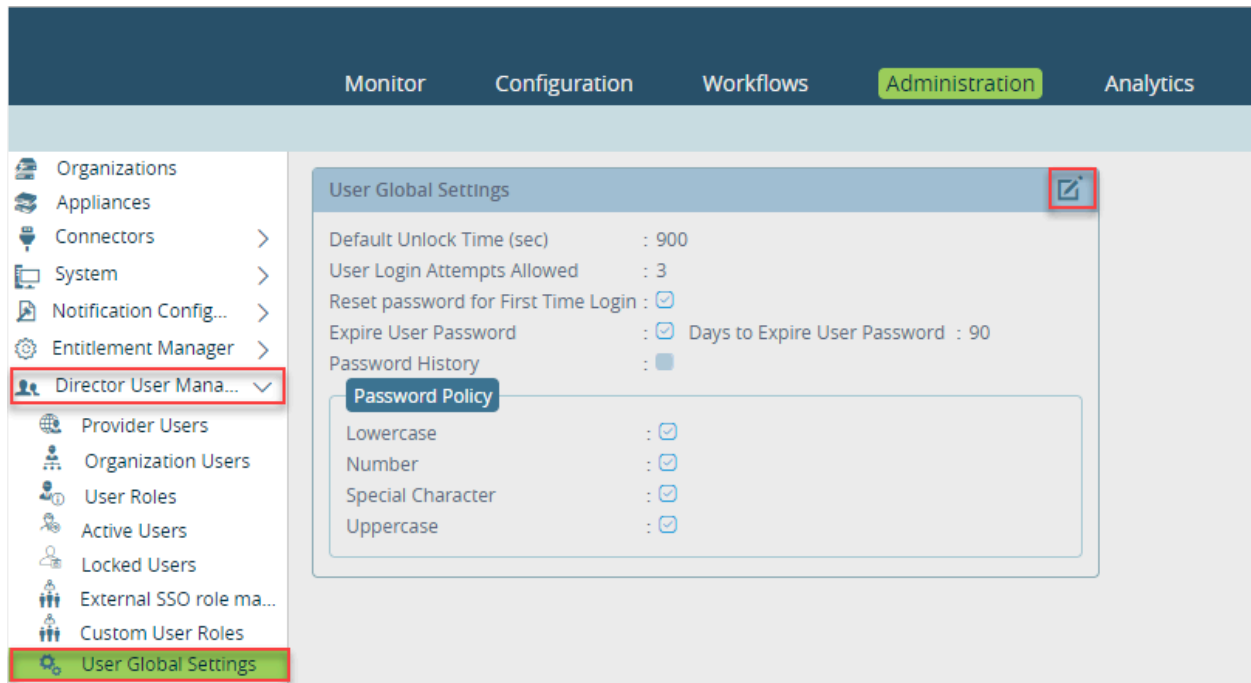
Modify Versa Director Account Password Complexity


You can configure the password properties for Director accounts, including the password complexity (that is, the types of characters the password must contain), how long passwords are valid, and how long previous passwords are remembered before they can be reused.

Note that changing Versa Director password complexity does not affect TACACS+ and RADIUS authentication policies, which are separate policies.

To edit the Versa Director password complexity:

1. In Director view, select the Administration tab in the top menu bar.
2. Select Director User Management > User Global Settings in the left menu bar.



3. Click the  Edit icon. In the Edit User Global Settings popup window, enter information for the following fields.

The 'Edit User Global Settings' popup window is shown with the following fields and options:

- Default Unlock Time (sec)*?**: Input field with value 900.
- User Login Attempts Allowed*?**: Input field with value 3.
- Reset password for First Time Login**: Checked checkbox.
- Password Policy** (grouped box):
 - Lowercase: Checked checkbox
 - Number: Checked checkbox
 - Special Character: Checked checkbox
 - Uppercase: Checked checkbox
 - Password Dictionary: Checked checkbox
- Expire User Password**: Checked checkbox.
 - Days to Expire User Password**: Input field with value 90.
- Password History**: Checked checkbox.
 - Password History Size**: Input field with value 3.

At the bottom of the window are 'OK' and 'Cancel' buttons.

Field	Description
Default Unlock Time	Enter the default unlock time, in seconds. If a user enters the wrong password too many times and is locked out, the user's account is unlocked after this amount of time has passed. <i>Default: 900 seconds</i>
User Login Attempts Allowed	Enter the number of user login attempts that are allowed before the user's account access is locked. Configuring a greater number of login attempts can help to protect against brute force login attacks. <i>Default: 3</i>
Reset Password for First-Time Login	Click to prompt the user to reset their password when they log in to the Director node for the first time.
Password Policy	Click one or more items to define the password complexity requirements.
Expire User Password	Click to have the user's password expire.
<ul style="list-style-type: none"> Days to Expire User Password 	Enter the number of days to use a password before it expires. <i>Default: 90 days</i>
Password History	Click to store the password history.
<ul style="list-style-type: none"> Password History Size 	Enter the number of past passwords that the user is not allowed to reuse. <i>Default: 3</i>

4. Click OK.

Enable SSH Banners

1. Copy the banner text to the /opt/versa/etc/banner.net file.
2. Change the file ownership to versa:versa:

```
| admin@director1:~$ sudo chown versa:versa /opt/versa/etc/banner.net
```

3. Replace the SSH banner with the text in the banner.net file:

```
| admin@director1$ sudo sed -i -e 's/#Banner.*/Banner Vopt\versa\etc\banner.net/' /etc/ssh/sshd_
config
```

4. Restart the SSH service:

```
| admin@director1$ sudo service ssh restart
```

Secure Communication Between Director HA Nodes

To provide additional hardening in a Director high availability (HA) architecture, you can encrypt the HA communication between Director instances.

You do not need to perform the procedure in this section if you used the secure communications option when you ran the Director setup script.

To secure communication between two Director HA nodes:

1. Secure the active Director instance by running the `secure-utils.sh` script on the primary Director node. For example:

```
| [Administrator@s2-vd-1: ~] $ sudo /opt/versa/vnms/scripts/secure-utils.sh --secure-ha-channel enable --psk test123  
=> Setting up strongSwan ipsec configuration..  
=> Restarting ipsec service..  
=> Done.
```

2. Secure the backup Director instance by running the `secure-utils.sh` script on the secondary Director node. For example:

```
| [Administrator@s2-vd-2: ~] $ sudo /opt/versa/vnms/scripts/secure-utils.sh --secure-ha-channel enable --psk test123  
=> Setting up strongSwan ipsec configuration..  
=> Restarting ipsec service..  
=> Done.
```

3. Verify that the communication is secure:

```
| [Administrator@s2-vd-1: ~] $ sudo ipsec statusall  
Status of IKE charon daemon (strongSwan 5.1.2, Linux 4.4.0-130-generic, x86_64):  
uptime: 17 minutes, since Aug 04 20:27:23 2019
```

Secure HA Ports

Harden Ports 4566, 4570, and 5432

Ports 4566, 4570, and 5432 are used to pair Director nodes for HA. To harden these ports, run the `secure-utils.sh` script on the primary and secondary Director nodes after you enable HA. This script modifies the iptables rules to deny access to the ports except for peer node IP addresses in the HA setup.

Before you harden HA ports, make sure you have the latest secure-utils.sh script. To update the script, issue the **sudo cp secure-utils.sh /opt/versa/vnms/scripts/** command.

To harden HA ports 4566, 4570, and 5432:

1. Run the secure-utils.sh script on the the active Director instance:

```
[Administrator@s2-vd-1: ~] $ sudo /opt/versa/vnms/scripts/secure-utils.sh --secure-ha-ports enable
```

The following is sample output from this command:

```
=> HA is enabled..
=> Peer Director's IP address is: 10.192.36.171
=> Setting up iptables rules
=> Create custom chain "vnmsha"
=> Allow access to port 4566, 4570, 5432 for 127.0.0.1
=> Allow access to port 4566, 4570, 5432 for 10.192.36.171
=> Allow access to port 4566, 4570, 5432 for 10.192.36.170
=> Disallow access to port 4566, 4570, 5432 for other IPs
=> Persist iptable rules and reload..
=> Done.
```

2. Run the secure-utils.sh script on the backup Director instance:

```
[Administrator@s2-vd-2: ~] $ sudo /opt/versa/vnms/scripts/secure-utils.sh --secure-ha-ports enable
```

The following is sample output from this command:

```
=> HA is enabled..
=> Peer Director's IP address is: 10.192.36.170
=> Setting up iptables rules
=> Create custom chain "vnmsha"
=> Allow access to port 4566, 4570, 5432 for 127.0.0.1
=> Allow access to port 4566, 4570, 5432 for 10.192.36.170
=> Allow access to port 4566, 4570, 5432 for 10.192.36.171
=> Disallow access to port 4566, 4570, 5432 for other IPs
=> Persist iptable rules and reload..
=> Done.
```

Change Default Passwords for Linux

Change the default passwords on both Director nodes for Linux users admin and Administrator. See [Change the Default Device Linux Passwords](#), below.

Change Default Passwords for Director

Change the default passwords on both Director nodes for Director users Administrator and Operator using the Director UI. See the [Change Default Passwords](#) section in Perform Initial Software Configuration.

Change the Default Passwords for the Postgres Database

Change the following passwords for the Postgres database from the default passwords on the primary Director node:

- Postgres user password
- VNMS user password

To change the Postgres user password:

1. Issue the following command on the primary Director node:

```
admin@Director-1:~$ password=$(tr -dc 'A-Za-z0-9!?!%*#%' < /dev/urandom | head -c 10) && sudo -S -u < <(echo 'versa123') postgres psql -c "alter role postgres with password '$password'" && echo "Password for 'postgres' user is $password"
```

2. Make a note of the newly generated password.

To change the VNMS user password:

1. Issue the following CLI command on the primary Director node:

```
admin@Director% set nms provider defaults database-credentials password password
```

2. Issue the **vsh restart** command to restart all services on both the primary and the secondary Director nodes:

```
admin@Director$ vsh restart
```

Disable Shell-in-a-Box

The Director shell-in-a-box function allows direct CLI access to the Director node and shell access to Versa Operating System™ (VOS™) devices from the Director GUI. You may want to disable this function, depending on your internal security policies.

When shell-in-a-box is enabled for VOS devices (appliances), users can access a shell login prompt by going to Administration > Appliances, clicking the box to the left of an appliance, and then selecting the Shell icon. Users must enter a valid shell account name and password to login to the shell.

When shell-in-a-box is enabled for a Director node, users can access the Versa CLI on the Director node by selecting Director CLI from the drop-down list in the upper right corner of the Director GUI. Users enter their Director user password to access the CLI.

To disable shell-in-a-box for Director and VOS devices:

1. Log in to the shell on the Director node. The default shell account is admin with password versa123.
2. Start the CLI:

```
admin@Director$ cli
```


3. Enter configuration mode:

```
| admin@Director> config
```

4. Disable the shell-in-a-box function by issuing the commands below. The first command disables shell login access to appliances from the Director GUI. The second disables CLI access to the Director node from the Director GUI.

```
| admin@Director% set system enable-appliance-shell-access false
| admin@Director% set system enable-director-shell-access false
```

5. Save the changes:

```
| admin@Director% commit
```

Update Security Packages

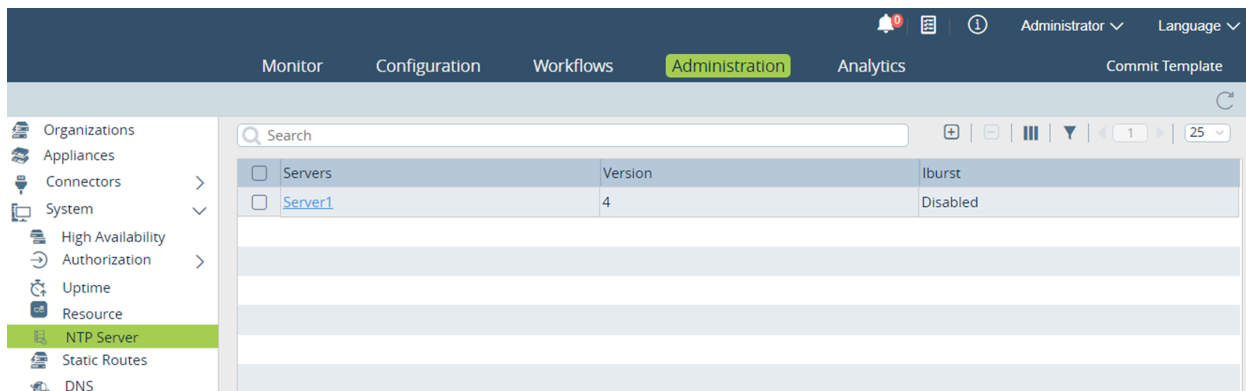
To harden the Director security, regularly update the Director nodes to the latest security pack (SPack). For more information, see [Use Security Packages](#).

Configure Time

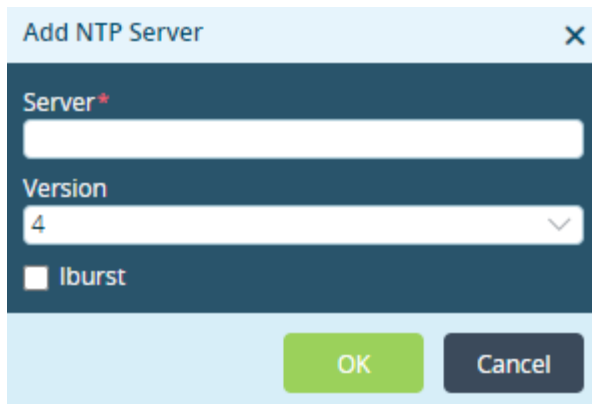
You configure the Network Time Protocol (NTP) and the timezone to use in the network so that all devices in the network operate on the same time. Time synchronization is important so that the timestamps in log files match across all devices. Also, there are cryptographic requirements for time synchronization.

To configure an NTP server:

1. In Director view, select the Administration tab in the top menu bar.
2. Select System > NTP Server in the left menu bar.



3. Click the Add icon. In the Add NTP Server popup window, enter the IP address of the NTP server. For more information, see [Configure an NTP Server](#).



Add NTP Server [X]

Server*

Version

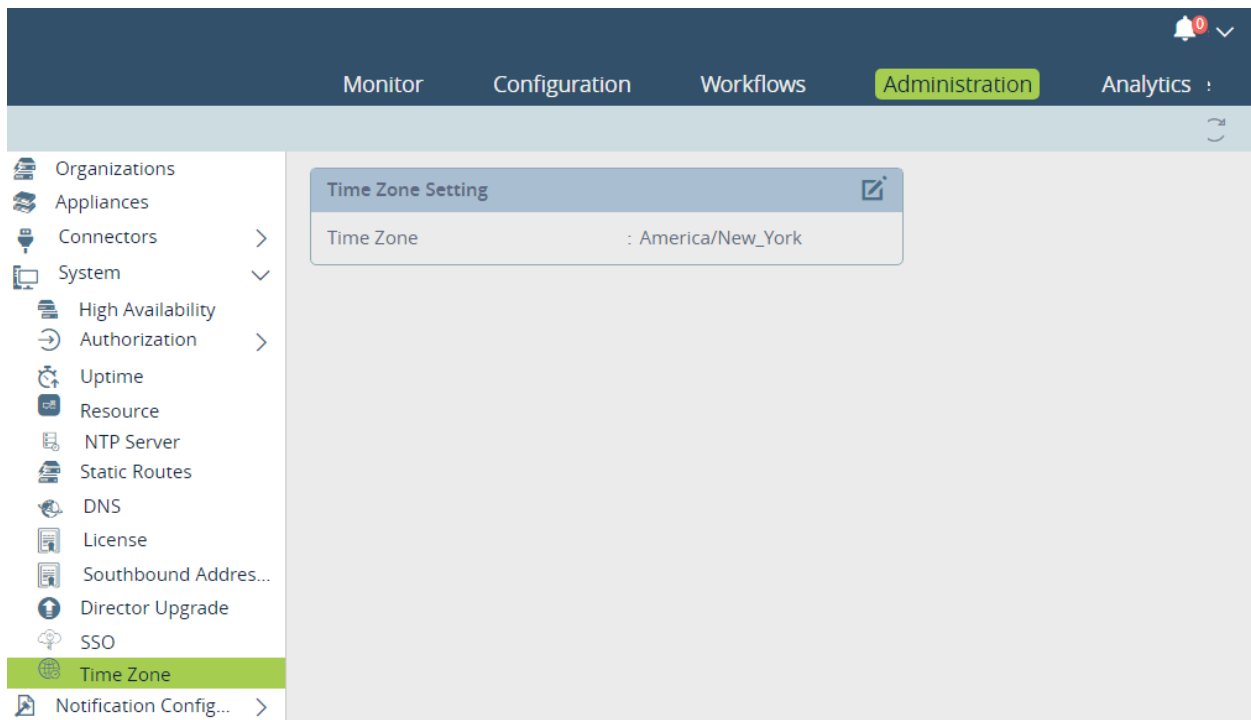
☐ lburst

OK Cancel

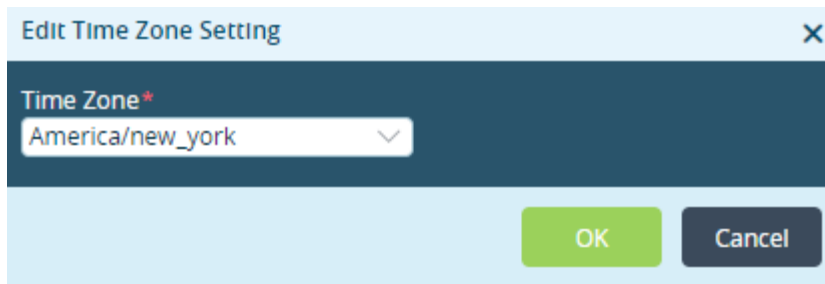
4. Click OK.

To configure the system timezone:

1. In Director view, select the Administration tab in the top menu bar.
2. Select System > Timezone in the left menu bar.



3. Click the  Edit icon.




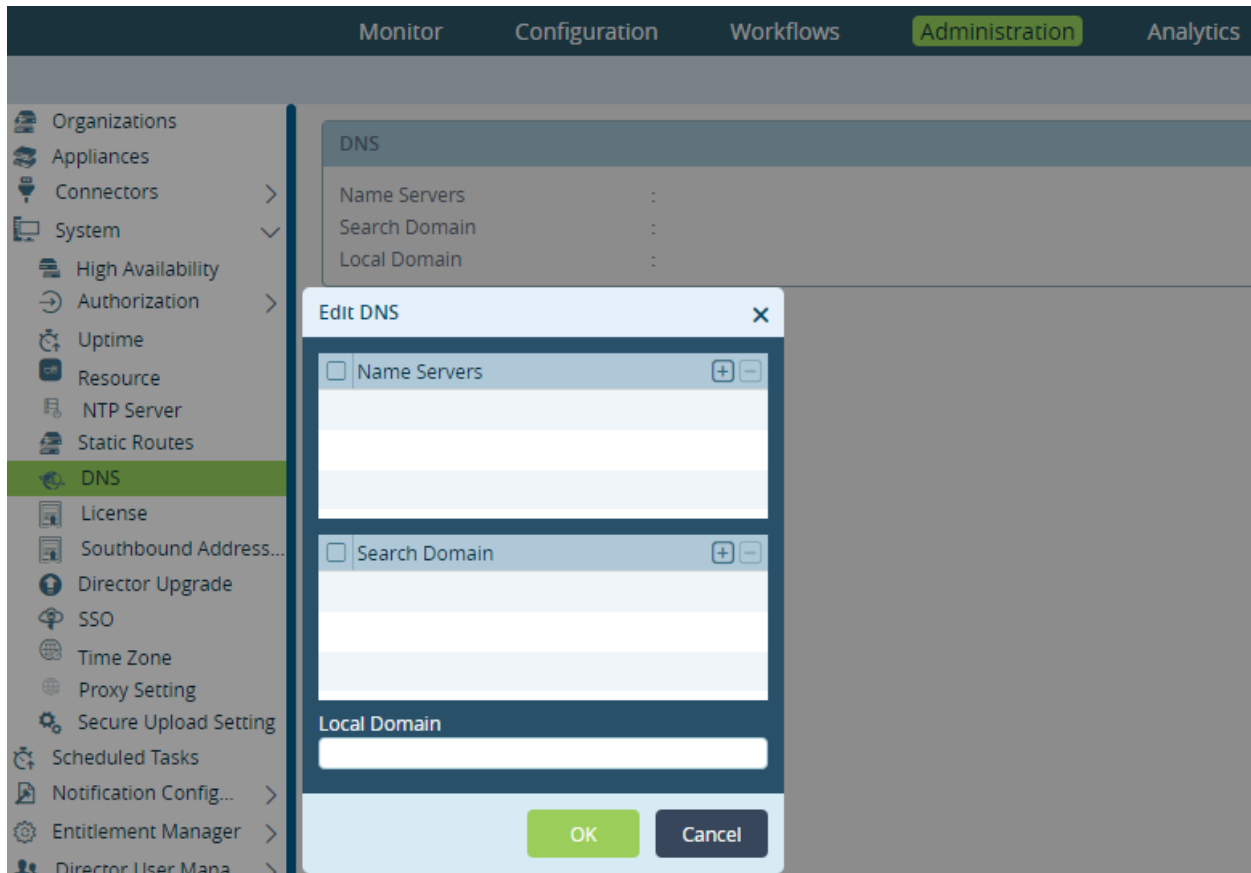
4. In the Edit Timezone setting popup window, select the time. For more information, see [Configure an NTP Server](#).
5. Click OK.

Configure DNS Servers

Many security exploits rely on injecting invalid Domain Name System (DNS) servers into the device to redirect resolution queries to a foreign DNS server. The DNS configuration described here forces a DNS server to be input to the device template to reduce DNS-based attacks.

To configure a DNS server:

1. In Director view, select the Administration tab in the top menu bar.
2. Select System > DNS in the left menu bar.
3. Click the  Edit icon.
4. In the Edit DNS popup window, enter the names of the allowed DNS servers. For more information, see [Configure a DNS Server](#).



5. Click OK.

Verify the Software Version

For the best performance of all SD-WAN components, Versa Networks requires that all components run the same software version.

To verify the software versions running on each network component:

1. To verify the software version of Versa Director or Analytics, log in to the CLI and issue the **show system package-info** CLI command. For example:

```
Administrator@director1> show system package-info
Package      Versa Director Software
Release     16.1R2
Build       S9
Release date 20190628
Package id   a454c1d
UI Package id 3580b52
Package name versa-director-20190628-150633-a454c1d-16.1R2S9
Branch      16.1R2
```

2. To verify the software version running on VOS devices:
 - a. In Director view, select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar. The Software Version column displays the version.

Monitor

Configuration

Workflows

Administration

Analytics

Organizations

Appliances

Connectors

System

High Availability

Authorization

Uptime

Resource

NTP Server

Static Routes

DNS

License

Southbound Address...

Total Appliances : 5

Search

	Name	Mgmt. Address	Type	Time Created	Service Start Time	Software Version	Site ID	Organizations
<input type="checkbox"/>	Branch-1	10.0.192.101	Branch	Wed, Nov 13 2019, ...	Thu, Dec 12 2019, ...	16.1-R2-S9	101	provider
<input type="checkbox"/>	Branch-2	10.0.192.102	Branch	Wed, Nov 13 2019, ...	Thu, Dec 12 2019, ...	16.1-R2-S9	102	provider
<input type="checkbox"/>	Branch-3	10.0.192.103	Branch	Wed, Nov 13 2019, ...	Thu, Dec 12 2019, ...	16.1-R2-S9	103	provider
<input type="checkbox"/>	Controller-1	10.48.61.13	Controller	Wed, Nov 13 2019, ...	Thu, Dec 12 2019, ...	16.1-R2-S9	1	provider
<input type="checkbox"/>	Controller-2	10.48.61.14	Controller	Wed, Nov 13 2019, ...	Thu, Dec 12 2019, ...	16.1-R2-S9	2	provider

Enable Centralized Authentication

It is recommended that you enable centralized authentication using TACACS+ or RADIUS on all Versa devices.

To enable centralized authentication:

1. In Director view, select the Administration tab in the top menu bar.
2. Select Connectors > Authentication in the left menu bar. The Authentication screen displays.

Monitor

Configuration

Workflows

Administration

Analytics

Commit Template

Organizations

Appliances

Connectors

Local

CMS

Authentication

Syslog

Kafka

AMQP

Analytics Cluster

Configuration

Service Name: test

Auth-order: remote-then-local

Retry Count: 3

Interval: 1

Expiry Time: 15

Default Connector

Default Connector :

Authentication Connectors

Search

Name	Type	IP Address	Port	Default IDP Connector
No Row Added				

3. Click the  Add icon in the Authentication Connectors pane to add an authentication connector.

Name*

☐ LDAP
 ☒ Radius
 ☐ Tacacs
 ☐ Active Directory

IP Address/FQDN	Port	Base DN	Bind DN
No Row Added			

☐ Default IDP Connector

Save Cancel

4. Select RADIUS or TACACS+ and enter the required information. For more information, see [Configure Authentication Connectors](#).
5. Click OK.

Authentication Attributes for SSH Access

To retain SSH access to a Director node, the following attributes must be returned as part of the TACACS+ or RADIUS accept message:

Attribute	Access Level
ProviderDataCenterAdmin	CLI read/write access
ProviderDataCenterOperator	CLI read only access

The following is a sample of a TACACS+ server configuration file:

```

root@tacacs:/etc/tacacs+# more tac_plus.conf
# See man(5) tac_plus.conf for more details

# Define where to log accounting data, this is the default.
accounting file = /var/log/tac_plus.acct

# This is the key that clients have to use to access Tacacs+
key = versa123

# Use /etc/passwd file to do authentication
#default authentication = file /etc/passwd

# You can use features like per-host key with different enable passwords

```

```

#host = 127.0.0.1 {
#    key = test
#    type = cisco
#    enable = <des|cleartext> enablepass
#    prompt = "Welcome XXX ISP Access Router \n\nUsername:"
# }

# You can define local users and specify a file where data is stored.
# That file may be filled using tac_pwd
# user = test1 {
#     name = "Test User"
#     member = staff
#     login = file /etc/tacacs/tacacs_passwords
# }

# You can specify rules valid per group of users.
# group = group1 {
#     cmd = conf {
#         deny
#     }
# }

# Another example : forbid configure command for some hosts for a defined range of clients
# group = group1 {
#     login = PAM
#     service = ppp
#     protocol = ip {
#         addr = 10.10.0.0/24
#     }
#     cmd = conf {
#         deny .*
#     }
# }

user = DEFAULT {
    login = PAM
    service = ppp protocol = ip {}
}

# Many more features are available, such as ACLs, more service compatibilities,
# commands authorization, scripting authorization.
# See the man page for these features.

group = TenantSuperAdminGroup {
    login = PAM
    service = test {
        Versa-Role = "TenantSuperAdmin"
        Versa-Tenant = "Galaxy-Foods"
        Versa-GUI-Idle-TimeOut = "300"
    }
}

group = TenantOperatorGroup {
    login = PAM

```

```

    service = test {
        Versa-Role = "TenantOperator"
        Versa-Tenant = "Galaxy-Foods"
        Versa-GUI-Idle-TimeOut = "300"
    }
}

group = TenantSecurityAdminGroup {
    login = PAM service = test {
        Versa-Role = "TenantSecurityAdmin"
        Versa-Tenant = "Galaxy-Foods"
        Versa-GUI-Idle-TimeOut = "300"
    }
}

group = TenantADCAdminGroup {
    login = PAM
    service = test {
        Versa-Role = "TenantADCAdmin"
        Versa-Tenant = "Galaxy-Foods"
        Versa-GUI-Idle-TimeOut = "300"
    }
}

group = ProviderDataCenterAdminGroup {
    login = PAM
    service = test {
        Versa-Role = "ProviderDataCenterAdmin"
        Versa-GUI-Idle-TimeOut = "300"
    }
}

group = ProviderDataCenterOperatorGroup {
    login = PAM service = test {
        Versa-Role = "ProviderDataCenterOperator"
        Versa-GUI-Idle-TimeOut = "300"
    }
}

group = ProviderDataCenterSystemAdminGroup {
    login = PAM service = test {
        Versa-Role = "ProviderDataCenterSystemAdmin"
        Versa-GUI-Idle-TimeOut = "300"
    }
}

group = flex_oper {
    default service = permit
    service = versa {
        Versa-User-Group = oper
    }
}

group = flex_admin {

```



```

    default service = permit
    service = versa {
        Versa-User-Group = admin
    }
}

group = uber_admin {
    default service = permit
    service = versa {
        Versa-User-Group = admin
    }
    login = PAM service = test {
        Versa-Role = "ProviderDataCenterSystemAdmin"
        Versa-GUI-Idle-TimeOut = "300"
    }
}

user = providersystemadmin {
    member = ProviderDataCenterSystemAdminGroup
    login = cleartext "versa123"
    pap = cleartext "versa123"
    # pap is needed for CLI access
    # # login is needed for GUI access
}

user = dave {
    default service = permit
    member = uber_admin
    login = des 1V4lf5pe4zRkE
    expires = "Sep 30 2099"
    pap = cleartext "versa123"
    # pap is needed for CLI access
    # # login is needed for GUI access
}

user = sultan {
    default service = permit
    member = ProviderDataCenterSystemAdminGroup
    login = des 1V4lf5pe4zRkE
    expires = "Sep 30 2099"
    pap = cleartext "versa123"
}

user = flexadmin {
    member = flex_admin
    login = cleartext "versa123"
    pap = cleartext "versa123"
}

```

Enable Secure Mode

You enable secure mode to harden the Linux core OS components to meet the Linux CIS benchmarks.

Before you enable secure mode, do the following:

- Download a full security package (SPack) and the SPack in the Versa Director so that the secure mode scripts are available. For more information, see [Use Security Packages](#).
- Enable centralized authentication. For more information, see [Enable Centralized Authentication](#), above.

To enable secure mode:

1. From the CLI, execute the secure-mode script:

```
| Administrator@director1> request system secure-mode enable
```

For example:

```
| Administrator@director1> request system secure-mode enable
Will enable secure mode. Are you sure? [no,yes] : yes
status success
result Enabling Versa OS secure mode
result Hardening SSH service
result Hardening password scheme
result Disabling USB storage
result Enabling system performance monitoring
result Hardening permissions on sensitive files
result Hardening: Disabling FileSystem knobs
result Hardening: Restricting the use of job-scheduling privilege
result Hardening: System knobs and TCP settings
result Hardening: Shadow users
result Hardening console login permissions
```

2. Exit the CLI and restart Versa services for the changes to take effect:

```
| admin@director1:~$ vsh restart
```

3. Change the Linux user passwords on the local device so that they all meet the complexity criteria.

To verify that secure mode is operating:

1. Issue the **request system secure-mode test brief** CLI command
2. Check the results in the `/var/log/versa/versa-security-test-date.log` file. The following is a sample of the log file contents that indicate that secure mode is operating properly:

```
| [admin@director1: ~] $ sudo cat /var/log/versa/versa-security-test-20190411-092258.log
[sudo] password for admin:
[INFO] sshd config check complete - error count = 0
[INFO] login.defs config check complete - error count = 0
[INFO] pam passwd config check complete - error count = 0
[INFO] blacklist config check complete - error count = 0
```

```
[ERROR] Default password found in file (/opt/versa/scripts/strongswan/get_ipsec_params.lua)
[INFO] Default password check complete - error count = 1
```

Update IP Tables

You update the Linux IP tables to define IP packet filter rules for the Linux kernel firewall that allow or block traffic to the system. When a connection tries to establish itself on the system, iptables looks for a rule in its list to match it to. If no rule is found, the default action is taken.

To create iptables rules:

1. Create the following iptables rules so that Director nodes can work properly, by allowing traffic to the following host interfaces:

- Primary and secondary Director northbound interface address
- Primary and secondary Director southbound interface address
- All Analytics northbound interface addresses
- All Analytics southbound interface addresses
- All third-party hosts that are using the Director REST API

```
sudo iptables -A INPUT -s ip-address -p tcp -m tcp --dport 9182 -j ACCEPT
sudo iptables -A INPUT -s ip-address -p tcp -m tcp --dport 9183 -j ACCEPT
sudo iptables -A INPUT -s ip-address -p tcp -m tcp --dport 20514 -j ACCEPT
```

2. Create the following iptables rules for internal communication to work correctly, by allowing traffic to the following host interfaces:

```
sudo iptables -A INPUT -s 127.0.0.1 -j ACCEPT
```

3. Create the following iptables rules for the external web service communications to work correctly, by allowing traffic to the following host interfaces:

```
sudo iptables -A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
sudo iptables -A INPUT -p tcp -m tcp --dport 8443 -j ACCEPT
```

4. Create the following iptables rules to block all outside traffic:

```
sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
sudo iptables -P OUTPUT ACCEPT
sudo iptables -P FORWARD DROP
sudo iptables -P INPUT DROP
```

5. Add rules for hosts requiring SSH access to the Director node:

```
sudo iptables -A INPUT -s ip-address-of-ssh-source -p tcp -m tcp --dport 22 -j ACCEPT
```

6. Save the iptables rules:

```
root@director1:~# iptables-save > /etc/iptables/rules.v4
```

Change the Default Device Linux Passwords

As part of the security hardening process, you must change the default Linux passwords of the following Director built-in user accounts:

- admin
- Administrator
- versa

To change the default passwords from the CLI:

1. Log in to the Director node as the admin user using the shell.
2. Change the admin user account password:

```
admin@director1:~$ passwd
Changing password for admin.
(current) UNIX password:
New password:
Retype new password:
passwd: password updated successfully
```

3. Change the versa user account password:

```
admin@director1:~$ sudo su versa
versa@director1:/home/admin$ passwd
Changing password for versa.
(current) UNIX password:
New password:
Retype new password:
passwd: password updated successfully
versa@director1:/home/admin$ exit
```

4. Change the Administrator user account password:

```
admin@director1:~$ sudo su Administrator
[aaaadmin@director1 admin] # passwd
Changing password for Administrator.
(current) UNIX password:
New password:
Retype new password:
passwd: password updated successfully
```

Disable Unused Kernel Modules

As part of Director hardening, you should disable the following unused Linux kernel modules to protect the device against the exploitation of any flaws in its implementation:

- DCCP—Datagram Congestion Control Protocol

- SCTP—Stream Control Transmission Protocol
- TDS—Tabular Data Stream protocol
- TIPC—Transparent Interprocess Communication protocol

To disable the unused kernel modules:

1. Edit the `/etc/modprobe.d/CIS.conf` file. Note that the file may not be present on the device.

```
# sudo vi /etc/modprobe.d/CIS.conf
```

2. Add the following lines to the file. The `/bin/true` option disables the loading of the kernel module.

```
install dccp /bin/true
install sctp /bin/true
install tds /bin/true
install tipc /bin/true
```

3. Save the file.
4. Check that the modules have been disabled:

```
# modprobe -n -v dccp
install /bin/true
# modprobe -n -v sctp
install /bin/true
# modprobe -n -v tds
install /bin/true
# modprobe -n -v tipc
install /bin/true
```

Disable Promiscuous Mode

As part of Director hardening, you should disable promiscuous mode on the `eth0` and `eth1` Ethernet interfaces.

To disable promiscuous mode on the `eth0` and `eth1` Ethernet interfaces:

1. Edit the `/etc/network/interfaces` file.

```
$ sudo vi /etc/network/interfaces
```

2. Locate the line `"iface ethx inet "`, and replace `x` with the interface number.
3. Add the line `"up ip link set ethx promisc off"` to the file, replacing `x` with the interface number.
4. Save the file.
5. Switch off promiscuous mode:

```
$ sudo ip link ethx promisc off
```

The following shows an example of the modified `/etc/network/interfaces` file for the `eth1` interface:

```
auto eth1
```

```
iface eth1 inet static
up ip link set eth1 promisc off
address 192.168.0.10
netmask 255.255.255.0
mtu 1200
up route add -net 192.168.0.0 netmask 255.255.0.0 gw 192.168.0.239
up route add -net 10.0.0.0 netmask 255.255.0.0 gw 192.168.0.239
up route add -net 10.1.0.0 netmask 255.255.0.0 gw 192.168.0.239
up route add -net 10.2.0.0 netmask 255.255.0.0 gw 192.168.0.239
```

Harden SSH

Change the SSH Port

To change the default port on which the SSH daemon listens:

1. Change the default SSH port:

```
$ sudo sed -i 's/22/1022/g' /etc/ssh/sshd_config
```

2. Restart the SSH service:

```
$ sudo service ssh restart
```

Disable the SSH Server

As part of system hardening, you can optionally disable the SSH service on the Director node.

To disable the SSH service:

1. Stop the SSH daemon:

```
$ sudo service ssh stop
```

2. Remove the SSH daemon from the init.d directory:

```
$ sudo rm /etc/init.d/ssh
```

Harden the SSH Server Configuration

To have the SSH server on the Director node continue to run, set the following parameters:

1. Edit the `/etc/ssh/sshd_config` file and replace the following values:
 - `ClientAliveInterval`—300
 - `ClientAliveCountMax`—0

2. Save the file.
3. Restart the SSH daemon:

```
| $ sudo service ssh restart
```

Disable strongSwan

To disable the strongSwan VPN on the Director node:

1. Stop the strongSwan service:

```
| $ sudo service strongswan stop > /dev/null 2>&1
```

2. Disable the service from starting when the Director node boots:

```
| $ update-rc.d -f strongswan remove > /dev/null 2>&1
```

Supported Software Information

Releases 20.2 and later support all content described in this article.

Additional Information

[Configure AAA](#)

[Configure Systemwide Functions](#)

[Perform Manual System Hardening for Versa Analytics](#)

[Perform Manual System Hardening for Versa Branches, Controllers, and Hubs](#)

[Use OS Security Package](#)