**Using This Master Template**

There are four sections on these first two pages that contain information on using the template:

* **Section 1 (IMPORTANT):** Seven fields immediately below in section 1 allow you to insert information specific to your document and then have that information AUTOMATICALLY populated into corresponding fields within the actual template below. This is a new capability that frees you up from having to update a document’s often-confusing Properties dialog window. Information in these fields is critical for ISO purposes.
* **Section 2:** Information on the Cisco Customer Experience (CX) *Documentation Master Template* and the accompanying *Documentation Style Guide*.
* **Section 3:** Information on updating a document’s security classification, if necessary. In most cases, this will not be necessary.
* **Section 4:** Information on updating a document’s footers, if necessary.
* These two template instruction pages, as well as other additional instructions (**red text**) on other pages of the template, ***must be removed*** before you submit a final document. Drag your mouse across all text and press ***Delete***. Be aware, you may have to press *Delete* twice to delete these first two pages.

**Section 1: Template’s Automatic Fields**

Click on a field below and then click on the small box with three dots appearing at the front of the field. This selects the field for updates. Enter an appropriate title for each of the seven fields. Corresponding fields within the actual template starting with the title page will now be automatically updated.

* [Project Name and Customer Name, e.g., “Cisco ACI for ABC Industries”]
* [Deliverable Name, e.g., “Low-Level Design”]
* [Version, e.g., “0.1”, “1.0”]
* [Author Name, e.g., “John Smith, Customer Experience, Cisco”]
* [Change Authority, e.g., “Customer Experience, Cisco”]
* [DCP Content ID, if applicable (otherwise “n/a”)]
* [Project ID, if applicable (otherwise “n/a”)]

**Section 2**: **Cisco CX Documentation** ***Master Template*** and ***Style Guide***

This Master Template presents a general framework of document sections that should be included in all documents of this type presented to the customer. Add or remove sections that fit your specific customer scenario. However, do not edit or remove the last two sections (Trademarks and Disclaimers, Document Acceptance) under any circumstances. The template is closely governed by instructions in the Cisco CX Documentation Style Guide mentioned below.

This template conforms to documentation style guidelines (fonts, headers, footers, format, graphics, etc.) included in all ICN templates, and it contains the ISO-required document control elements and the Cisco data classification as well. Please send any feedback or requests for style enhancements to the following:

[svt-templates-team@cisco.com](mailto:svt-templates-team@cisco.com)

* Click below to access a page containing a link to a PowerPoint deck on the DCP process as it relates to documentation standards in Cisco CX. It contains information on document requirements, templates, processing, reviews, approvals, versioning, etc.  
  <https://go2.cisco.com/DCP2DailyUse>

The Cisco CX Documentation **Style Guide** contains detailed instructions on document structure, formatting, styles, figures and tables, graphics, trademarks and disclaimers, and customer acceptance. The Style Guide can be found here: <https://docs.cisco.com/share/proxy/alfresco/url?docnum=EDCS-22030275&ver=approved>

It is essential writers review the Style Guide for instructions on properly writing their documents. Instructions in the guide are Cisco CX-approved and ISO-compliant.

**Section 3:** **Changing a Document’s** ***Security Classification*** **in the Footer**

This template allows an author to change the security classification appearing in the footer, from the default of Cisco Highly Confidential to Cisco Public, Cisco Confidential, or Cisco Restricted:

1. Go to **File** > **Info** > **Properties** > **Advanced Properties** > **Custom** tab.
2. In the Properties field, scroll to the bottom and click on **Document Classification.**
3. In the Value field immediately above, type a new classification level and click **Modify**.
4. Click **OK**.
5. See the instructions below for ***Updating a Document’s Page Footers*** to update the document’s classification.

|  |
| --- |
| For Apple Mac users:   1. From your Apple Mac’s main toolbar at the top of the screen, click on File and select Properties. 2. Click on Custom tab. 3. In the Properties field, click on Document Classification. 4. In the Value field immediately above, type a new classification level and click Modify. 5. Click OK. See the instructions below for *Updating a Document’s Page Footers* to update the document’s classification. |

For more information on *Security Classifications*: <http://wwwin.cisco.com/infosec/policies/classification.shtml>

**Section 4:** **Updating a Document’s** ***Page Footers***

1. Scroll to the first page displaying the standard expanded footer (as opposed to the abbreviated footer on the title page), which should be the first page of the Table of Contents.
2. Double-click anywhere in the footer. The Header and Footer tab automatically opens.
3. If you have changed the document’s default classification from **Cisco Highly Confidential** to one of the other accepted classifications, right-click on the classification field in the footer and select Update Field to update the footer.

Scroll down after the cover page to make sure the footer has been updated on subsequent pages in the document. If not, repeat the process on those pages and then recheck the footers again.



[Project Name and Customer Name, e.g., “Cisco ACI for ABC Industries”]

[Deliverable Name, e.g., “Low-Level Design”]

October 4, 2023

Version [Version, e.g., “0.1”, “1.0”]

Phone: +1 408-526-4000

Toll Free: +1 800-553-NETS (6387)

Fax: +1 408-526-4100

**Document Classification**

**Cisco Highly Confidential**

170 West Tasman Drive

San Jose, CA 95134-1706 USA

Cisco Systems, Inc.

Corporate Headquarters

Contents

[Contents 2](#_Toc95212150)

[List of Figures and Tables 3](#_Toc95212151)

[About This Document 4](#_Toc95212152)

[History 4](#_Toc95212153)

[Review 4](#_Toc95212154)

[Document Conventions 4](#_Toc95212155)

[1 Introduction 5](#_Toc95212156)

[1.1 Preface 5](#_Toc95212157)

[1.2 Audience 5](#_Toc95212158)

[1.3 Scope 5](#_Toc95212159)

[1.4 Assumptions 5](#_Toc95212160)

[1.5 Related Documents 5](#_Toc95212161)

[2 Heading 1 6](#_Toc95212162)

[2.1 Heading 2 6](#_Toc95212163)

[2.1.1 Heading 3 6](#_Toc95212164)

[Heading 1-No Numbers 7](#_Toc95212165)

[Heading 2-No Numbers 7](#_Toc95212166)

[Heading 3-No Numbers 7](#_Toc95212167)

[3 Appendix A: Title 8](#_Toc95212168)

[3.1 Appendix A Sub-Section 8](#_Toc95212169)

[3.1.1 Appendix A Sub-Section 8](#_Toc95212170)

[4 Appendix B: Acronym Listing/Glossary 9](#_Toc95212171)

[Trademarks and Disclaimers 10](#_Toc95212172)

[Document Acceptance 11](#_Toc95212173)

List of Figures and Tables

**No table of figures entries found.**

**No table of figures entries found.**

About This Document

|  |  |
| --- | --- |
| Author | [Author Name, e.g., “John Smith, Customer Experience, Cisco”] |
| Change Authority | [Change Authority, e.g., “Customer Experience, Cisco”] |
| DCP Reference | [DCP Content ID, if applicable (otherwise “n/a”)] |
| Project ID | [Project ID, if applicable (otherwise “n/a”)] |

History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Status | Change Description |
| 0.1 | YYYY-MM-DD | Pre-draft | Initial creation |
| 0.2 |  |  |  |
| 0.3 |  |  |  |
| … |  | Draft |  |
| 1.0 |  | Final |  |

Review

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Reviewer | Review Description |
| 0.x | YYYY-MM-DD |  |  |
| … |  |  |  |
| … |  |  |  |

Document Conventions

|  |  |
| --- | --- |
|  | Caution: Alerts readers to be careful. In this situation, you might do something that could result in equipment damage or loss of data. |
|  | Note: Alerts readers to take note. Notes contain helpful suggestions or references to material not covered in the document. |
|  | Timesaver: Alerts the reader that they can save time by performing the action described in the paragraph affixed to this icon. |
|  | Tip: Alerts the reader that the information affixed to this icon will help them solve a problem. The information might not be troubleshooting or even an action, but it could be useful information similar to a Timesaver. |
|  | Warning: Alerts readers of a situation that could cause bodily injury. They need to be aware of the hazards involved with electrical circuitry and familiarize themselves with standard practices for preventing accidents. |

# Introduction

## Preface

[Enter appropriate text in this section using style **Normal**.]

## Audience

[Enter appropriate text in this section using style **Normal**.]

## Scope

[Enter appropriate text in this section using style **Normal**.]

## Assumptions

[Enter appropriate text in this section using style **Normal**.]

## Related Documents

[Enter appropriate text in this section using style **Normal**.]

* It is absolutely essential writers review the Cisco CX Documentation Style Guide for instructions on properly writing their documents. Instructions in the guide are Cisco CX-approved and ISO-compliant. Adherence to the Style Guide is mandatory. The Style Guide is available in Doc Central:   
  <https://docs.cisco.com/share/proxy/alfresco/url?docnum=EDCS-22030275&ver=approved>

# Heading 1

[Enter appropriate text in this section using style **Normal**.]

## Heading 2

[Enter appropriate text in this section using style **Normal**.]

### Heading 3

[Enter appropriate text in this section using style **Normal**.]

#### Heading 4

[Enter appropriate text in this section using style **Normal**.]

##### Heading 5

[Enter appropriate text in this section using style **Normal**.]

###### Heading 6

[Enter appropriate text in this section using style **Normal**.]

Heading 7

[Enter appropriate text in this section using style **Normal**.]

Heading 8

[Enter appropriate text in this section using style **Normal**.]

Heading 9

[Enter appropriate text in this section using style **Normal**.]

1. AAA

Heading 1-No Numbers

[Enter appropriate text in this section using style **Normal**.]

* In using this Cisco CX Document Master Template, if for some reason you decide to use one of the unnumbered types of headings, you will be unable to set up cross-references from text in other numbered sections in your document to text in these unnumbered sections.

Heading 2-No Numbers

[Enter appropriate text in this section using style **Normal**.]

Heading 3-No Numbers

[Enter appropriate text in this section using style **Normal**.]

Heading 4-No Numbers

[Enter appropriate text in this section using style **Normal**.]

Heading 5-No Numbers

[Enter appropriate text in this section using style **Normal**.]

# Appendix A: Title

[Enter appropriate text in this section using style **Normal**.]

## Appendix A Sub-Section

[Enter appropriate text in this section using style **Normal**.]

### Appendix A Sub-Section

[Enter appropriate text in this section using style **Normal**.]

# Appendix B: Acronym Listing/Glossary

* Adjust the section headline depending on its content   
  (either "Appendix B: Acronym Listing" or "Appendix B: Glossary").

|  |  |
| --- | --- |
| Term | Definition |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Trademarks and Disclaimers

IF THIS DOCUMENT IS PROVIDED AS A DELIVERABLE IN ACCORDANCE WITH THE CISCO TERMS AND CONDITIONS ASSOCIATED WITH A PURCHASED CISCO SERVICE (“TERMS”) THEN THIS DOCUMENT IS PRESENTED SUBJECT TO THOSE TERMS. IN ALL OTHER EVENTS, THIS DOCUMENT IS PROVIDED “AS-IS” WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2022 Cisco and/or its affiliates. All rights reserved.

Document Acceptance

|  |  |  |  |
| --- | --- | --- | --- |
| Name |  | Name |  |
| Title |  | Title |  |
| Company |  | Company |  |
| Signature |  | Signature |  |
| Date |  | Date |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Name |  | Name |  |
| Title |  | Title |  |
| Company |  | Company |  |
| Signature |  | Signature |  |
| Date |  | Date |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Name |  | Name |  |
| Title |  | Title |  |
| Company |  | Company |  |
| Signature |  | Signature |  |
| Date |  | Date |  |

# Ncs Env

This set of tests validates the system envionment changes have been made for  
the Cisco NSO application and the T-SDN Core Function Pack the changes relate to:  
- overcommit\_memory disabled across reboots  
- system limits configured as per T-SDN package documentation

Table- Ncs Env Test Results Summary

|  |  |  |
| --- | --- | --- |
| pass | fail | skip |
| 3 | 0 | 0 |

Table- Verify that the overcommit\_memory value has been updated

|  |  |
| --- | --- |
| section | s1-s1 |
| Purpose | The default os value is pre-configured to 0, this needs to be modified to "2". This can be changed at run-time by "echo 2 > /proc/sys/vm/overcommit\_memmory" however it should be persistently added to the /etc/sysctl.d/ncs.conf this test will check both locations |
| procedure |  |
| status | PASS |
| messages | Running command 'cat /proc/sys/vm/overcommit\_memory 2>&1'. ${run\_time\_overcommit} = 2 Getting file '<a href="file:///etc/sysctl.d/ncs.conf">/etc/sysctl.d/ncs.conf</a>'. ${sysctl\_d\_ncs\_conf} = # Adding Over Commit Memmory Changes # This change keeps overcommit\_memmory (OOM) disbaled across system reboots. vm.overcommit\_memory = 2 ${error\_list} = [] /proc/sys/vm/overcommit\_memory is configured correctly ${matches} = ['2'] ['2'] 2 vm.overcommit\_memory assigned to correct values Length is 0 |

Table- Verify the T-SDN system limits have been configured

|  |  |
| --- | --- |
| section | s1-s1 |
| Purpose | The T-SDN Core Function Pack requires system limit changes to be made the test will check the /etc/security/limnits.d/ncs.conf file exists and that the expected values have been provided. The expected values are stored in a dict k,v arrangement and can be extended if needed To handle the Regex \* issue we need to preface each key with \\*s+ should be handled in the KEywork but thats for the future |
| procedure |  |
| status | PASS |
| messages | Getting file '<a href="file:///etc/security/limits.d/ncs.conf">/etc/security/limits.d/ncs.conf</a>'. ${file} = # Adding T-SDN System Limits needed for NSO \* soft nproc 65535 \* hard nproc 65535 \* soft nofile 65535 \* hard nofile 65535 \* hard memlock 65536 \* soft memlock 65536 ${clean\_file} = # Adding T-SDN System Limits needed for NSO \* soft nproc 65535 \* hard nproc 65535 \* soft nofile 65535 \* hard nofile 65535 \* hard memlock 65536 \* soft memlock 65536 ${limits\_dict} = {'soft nproc': '65535', 'hard nproc': '65535', 'soft nofile': '65535', 'hard memlock': '65536', 'soft memlock': '65536'} ${error\_list} = [] ${matches} = ['65535'] Length is 1 ${len} = 1 soft nproc value found, and set to the expected value : 65535 ${matches} = ['65535'] Length is 1 ${len} = 1 hard nproc value found, and set to the expected value : 65535 ${matches} = ['65535'] Length is 1 ${len} = 1 soft nofile value found, and set to the expected value : 65535 ${matches} = ['65536'] Length is 1 ${len} = 1 hard memlock value found, and set to the expected value : 65536 ${matches} = ['65536'] Length is 1 ${len} = 1 soft memlock value found, and set to the expected value : 65536 Length is 0 |

Table- Verify that the limit changes are applied to the system

|  |  |
| --- | --- |
| section | s1-s1 |
| Purpose | This test checks that the variables applied to the /etc/security/limits.d/ncs.conf have been applied. This typically requires a user to disconnect and reconnect to the servers |
| procedure |  |
| status | PASS |
| messages | Running command 'ulimit -a 2>&1'. ${ulimit\_settings} = real-time non-blocking time (microseconds, -R) unlimited core file size (blocks, -c) 0 data seg size (kbytes, -d) unlimited scheduling priority (-e) 0 file ... ${ulimit\_dict} = {'max locked memory': '65536', 'open files': '65535', 'max user processes': '65535'} ${error\_list} = [] max locked memory:65536 ${matches} = ['65536'] Length is 1 ${len} = 1 max locked memory value found, and set to the expected value : 65536 open files:65535 ${matches} = ['65535'] Length is 1 ${len} = 1 open files value found, and set to the expected value : 65535 max user processes:65535 ${matches} = ['65535'] Length is 1 ${len} = 1 max user processes value found, and set to the expected value : 65535 Length is 0 |

# Security

The following tests verify the security configuration that are expected to be implemented  
on the redhat servers that will host the Cisco NSO application  
- firewall Service Configrations  
- autheselect custome profile creation and modifications  
- PAM Configrations  
- Password quality modifications  
Refer to the SCDP documentation to address any failed tests.

Table- Security Test Results Summary

|  |  |  |
| --- | --- | --- |
| pass | fail | skip |
| 11 | 0 | 0 |

Table- Verify firewalld service is enabled

|  |  |
| --- | --- |
| section | s1-s2 |
| Purpose | The firewall service should not be disabled on reboot |
| procedure |  |
| status | PASS |
| messages | Running command 'systemctl is-enabled firewalld 2>&1'. ${output} = enabled |

Table- Verify NSO ports are configured in the firewalld

|  |  |
| --- | --- |
| section | s1-s2 |
| Purpose | Check that the neccesary tcp/udp ports are open for nso the ports are listed in the list "nso\_fw\_ports" defined in the global Variables List includes the following : ['2022', '2024', '8080', '8888'] |
| procedure |  |
| status | PASS |
| messages | Running command 'sudo firewall-cmd --list-all 2>&1'. ${output} = public (active) target: default icmp-block-inversion: no interfaces: ens33 sources: services: cockpit dhcpv6-client ssh ports: 22/tcp 4570/tcp 2022/tcp 2023/tcp 2024/tcp 8080/tcp 8888/tcp... 2022 2024 8080 8888 |

Table- Verify authselect profile sssd-vf is created

|  |  |
| --- | --- |
| section | s1-s2 |
| Purpose | Verify that a custom sssd profile has been created |
| procedure |  |
| status | PASS |
| messages | Running command 'authselect list 2>&1'. ${output} =  - minimal Local users only for minimal installations  - sssd Enable SSSD for system authentication (also for local users only)  - winbind Enable winbind for system authenticat... |

Table- Verify expected authselect profile is active

|  |  |
| --- | --- |
| section | s1-s2 |
| Purpose | This runs the command "authselect current -r" and returns the current active profile the test checks that this matches the expected value of custom/sssd-vf |
| procedure |  |
| status | PASS |
| messages | Running command 'authselect current -r 2>&1'. ${output} = custom/sssd-vf with-faillock without-nullok ${profile} = custom/sssd-vf Execution passed with message: Current Profile is correct  - sssd-vf |

Table- Verify that the required PAM Modules are enabled

|  |  |
| --- | --- |
| section | s1-s2 |
| Purpose | This test will verify that without-nullok and with-faillock modules are activated the test will run the command "autheselect current" which returns the enabled features in the format: Profile ID: custom/sssd-vf Enabled features:  - with-faillock  - without-nullok Checks made against the following features: ['with-faillock', 'without-nullok'] |
| procedure |  |
| status | PASS |
| messages | Running command 'authselect current 2>&1'. ${output} = Profile ID: custom/sssd-vf Enabled features:  - with-faillock  - without-nullok ${module\_status\_dict} = {} Profile ID: custom/sssd-vf Enabled features:  - with-faillock  - without-nullok ${regex\_result} = PASS ${regex\_message} = with-faillock ${regex\_result} = PASS ${regex\_message} = without-nullok {'with-faillock': 'PASS', 'without-nullok': 'PASS'} ${status} = PASS ${status\_message} = None PASS |

Table- Check the password-auth file has been updated

|  |  |
| --- | --- |
| section | s1-s2 |
| Purpose | Read the /etc/authselect/custom/sssd-vf/password-auth file and check that the values have been modified the check takes a dict with the module search string and the expected configuration as a k,v Pairs the check then searches the file for the key and evaluates the value |
| procedure |  |
| status | PASS |
| messages | ${check\_dict} = {'auth.\*pam\_unix.so': '{if not "without-nullok":nullok} try\_first\_pass', 'password.\*pam\_pwquality.so': 'try\_first\_pass local\_users\_only', 'password.\*pam\_unix.so sha512 shadow': '{if not "without-nullo... Getting file '<a href="file:///etc/authselect/custom/sssd-vf/password-auth">/etc/authselect/custom/sssd-vf/password-auth</a>'. ${password\_auth} = auth required pam\_env.so auth required pam\_faildelay.so delay=2000000 auth required ... ${error\_list} = [] auth.\*pam\_unix.so : {if not "without-nullok":nullok} try\_first\_pass ${matches} = ['{if not "without-nullok":nullok} try\_first\_pass'] Length is 1 ${len} = 1 Match Found match auth.\*pam\_unix.so : ['{if not "without-nullok":nullok} try\_first\_pass'] {if not "without-nullok":nullok} try\_first\_pass 'auth.\*pam\_unix.so' Configured as expected password.\*pam\_pwquality.so : try\_first\_pass local\_users\_only ${matches} = ['try\_first\_pass local\_users\_only'] Length is 1 ${len} = 1 Match Found match password.\*pam\_pwquality.so : ['try\_first\_pass local\_users\_only'] try\_first\_pass local\_users\_only 'password.\*pam\_pwquality.so' Configured as expected password.\*pam\_unix.so sha512 shadow : {if not "without-nullok":nullok} try\_first\_pass use\_authtok ${matches} = ['{if not "without-nullok":nullok} try\_first\_pass use\_authtok'] Length is 1 ${len} = 1 Match Found match password.\*pam\_unix.so sha512 shadow : ['{if not "without-nullok":nullok} try\_first\_pass use\_authtok'] {if not "without-nullok":nullok} try\_first\_pass use\_authtok 'password.\*pam\_unix.so sha512 shadow' Configured as expected [] Length is 0 |

Table- Check the system-auth file has been updated

|  |  |
| --- | --- |
| section | s1-s2 |
| Purpose | Read the /etc/authselect/custom/sssd-vf/system-auth file and check that the values have been modified the check takes a dict with the module search string and the expected configuration as a k,v Pairs the check then searches the file for the key and evaluates the value |
| procedure |  |
| status | PASS |
| messages | ${check\_dict} = {'auth.\*pam\_unix.so': '{if not "without-nullok":nullok} try\_first\_pass', 'password.\*pam\_pwquality.so': 'try\_first\_pass local\_users\_only enforce-for-root retry=3 remember=12', 'password.\*pam\_unix.so sh... Getting file '<a href="file:///etc/authselect/custom/sssd-vf/system-auth">/etc/authselect/custom/sssd-vf/system-auth</a>'. ${password\_auth} = {imply "with-smartcard" if "with-smartcard-required"} auth required pam\_env.so auth required pam\_faildelay.so dela... ${error\_list} = [] auth.\*pam\_unix.so : {if not "without-nullok":nullok} try\_first\_pass ${matches} = ['{if not "without-nullok":nullok} try\_first\_pass'] Length is 1 ${len} = 1 Match Found match auth.\*pam\_unix.so : ['{if not "without-nullok":nullok} try\_first\_pass'] {if not "without-nullok":nullok} try\_first\_pass auth.\*pam\_unix.so Configured as expected password.\*pam\_pwquality.so : try\_first\_pass local\_users\_only enforce-for-root retry=3 remember=12 ${matches} = ['try\_first\_pass local\_users\_only enforce-for-root retry=3 remember=12'] Length is 1 ${len} = 1 Match Found match password.\*pam\_pwquality.so : ['try\_first\_pass local\_users\_only enforce-for-root retry=3 remember=12'] try\_first\_pass local\_users\_only enforce-for-root retry=3 remember=12 password.\*pam\_pwquality.so Configured as expected password.\*pam\_unix.so sha512 shadow : {if not "without-nullok":nullok} try\_first\_pass use\_authtok remember=12 ${matches} = ['{if not "without-nullok":nullok} try\_first\_pass use\_authtok remember=12'] Length is 1 ${len} = 1 Match Found match password.\*pam\_unix.so sha512 shadow : ['{if not "without-nullok":nullok} try\_first\_pass use\_authtok remember=12'] {if not "without-nullok":nullok} try\_first\_pass use\_authtok remember=12 password.\*pam\_unix.so sha512 shadow Configured as expected [] Length is 0 |

Table- Verify that faillock.conf has been modifed

|  |  |
| --- | --- |
| section | s1-s2 |
| Purpose | We are required to modify the fail\_interval to be = 1800 seconds |
| procedure |  |
| status | PASS |
| messages | ${dict} = {'fail\_interval': '1800'} ${file\_path} = /etc/security/faillock.conf {'fail\_interval': '1800'} /etc/security/faillock.conf Getting file '<a href="file:///etc/security/faillock.conf">/etc/security/faillock.conf</a>'. ${file} = # Configuration for locking the user after multiple failed # authentication attempts. # # The directory where the user files with the failure records are kept. # The default is /var/run/faillock. # di... ${errors\_list} = [] ${match} = ['1800'] Length is 1 ${number\_of\_results} = 1 ${match\_val} = 1800 ${status} = PASS ${status\_message} = None Length is 0 |

Table- Verify that pwquality.conf has been modified

|  |  |
| --- | --- |
| section | s1-s2 |
| Purpose | We are required to modify the /etc/security/pwquality.conf to ensure only complex passwords are allowed following values should be used:  - minlen = 8  - dcredit = -1  - ucredit = -1  - lcredit = -1  - ocredit = -1 |
| procedure |  |
| status | PASS |
| messages | ${dict} = {'minlen': '8', 'dcredit': '-1', 'ucredit': '-1', 'lcredit': '-1', 'ocredit': '-1'} ${file\_path} = /etc/security/pwquality.conf {'minlen': '8', 'dcredit': '-1', 'ucredit': '-1', 'lcredit': '-1', 'ocredit': '-1'} /etc/security/pwquality.conf Getting file '<a href="file:///etc/security/pwquality.conf">/etc/security/pwquality.conf</a>'. ${file} = # Configuration for systemwide password quality limits # Defaults: # # Number of characters in the new password that must not be present in the # old password. # difok = 1 # # Minimum acceptable size ... ${errors\_list} = [] ${match} = ['8'] Length is 1 ${number\_of\_results} = 1 ${match\_val} = 8 ${status} = PASS ${status\_message} = None ${match} = ['-1'] Length is 1 ${number\_of\_results} = 1 ${match\_val} = -1 ${status} = PASS ${status\_message} = None ${match} = ['-1'] Length is 1 ${number\_of\_results} = 1 ${match\_val} = -1 ${status} = PASS ${status\_message} = None ${match} = ['-1'] Length is 1 ${number\_of\_results} = 1 ${match\_val} = -1 ${status} = PASS ${status\_message} = None ${match} = ['-1'] Length is 1 ${number\_of\_results} = 1 ${match\_val} = -1 ${status} = PASS ${status\_message} = None Length is 0 |

Table- Verify login.defs has been modifed

|  |  |
| --- | --- |
| section | s1-s2 |
| Purpose | Password expiration values need to be modified in the /etc/login.defs file the default values need to be modified to meet the following requirements:  - PASS\_MIN\_LEN 5  - PASS\_MAX\_DAYS 90  - PASS\_MIN\_DAYS 1  - PASS\_WARN\_AGE 5 |
| procedure |  |
| status | PASS |
| messages | ${dict} = {'PASS\_MAX\_DAYS': '90', 'PASS\_MIN\_DAYS': '1', 'PASS\_MIN\_LEN': '5', 'PASS\_WARN\_AGE': '5'} ${file\_path} = /etc/login.defs {'PASS\_MAX\_DAYS': '90', 'PASS\_MIN\_DAYS': '1', 'PASS\_MIN\_LEN': '5', 'PASS\_WARN\_AGE': '5'} /etc/login.defs Getting file '<a href="file:///etc/login.defs">/etc/login.defs</a>'. ${file} = # # Please note that the parameters in this configuration file control the # behavior of the tools from the shadow-utils component. None of these # tools uses the PAM mechanism, and the utilities that... ${errors\_list} = [] ${match} = ['90'] Length is 1 ${number\_of\_results} = 1 ${match\_val} = 90 ${status} = PASS ${status\_message} = None ${match} = ['1'] Length is 1 ${number\_of\_results} = 1 ${match\_val} = 1 ${status} = PASS ${status\_message} = None ${match} = ['5'] Length is 1 ${number\_of\_results} = 1 ${match\_val} = 5 ${status} = PASS ${status\_message} = None ${match} = ['5'] Length is 1 ${number\_of\_results} = 1 ${match\_val} = 5 ${status} = PASS ${status\_message} = None Length is 0 |

Table- Verify the user account inavtive days value has been modified

|  |  |
| --- | --- |
| section | s1-s2 |
| Purpose | The default value of INACTIVE in /etc/defaults/useradd is set to -1 which equates to no inactvity time out for user. We need to change this value to 90 as per request from Customer |
| procedure |  |
| status | PASS |
| messages | Getting file '<a href="file:///etc/default/useradd">/etc/default/useradd</a>'. ${useradd\_conf} = # useradd defaults file GROUP=100 HOME=/home INACTIVE=90 # INACTIVE=-1 EXPIRE= SHELL=/bin/bash SKEL=/etc/skel CREATE\_MAIL\_SPOOL=yes ${match} = ['90'] ${match\_val} = 90 |

# System

The following tests verify the operating system configuration & dependency packages  
are present in preperation for the Cisco NSO application testing. The checks include:  
- dependent packages are available  
- required utilities are present  
- hostname has been changed  
- DNS and NTP serviecs are configured and active  
  
Refer to the SCDP documentation to address any failed tests.

Table- System Test Results Summary

|  |  |  |
| --- | --- | --- |
| pass | fail | skip |
| 6 | 0 | 0 |

Table- Verify dependency packages are installed

|  |  |
| --- | --- |
| section | s1-s3 |
| Purpose | As above without break on first failure |
| procedure |  |
| status | PASS |
| messages | ${command} = rpm -q ${check\_string} = not installed ${errors\_list} = [] ${run\_cmd} = rpm -q ant rpm -q ant Running command 'rpm -q ant 2>&1'. ${output} = ant-1.10.9-7.el9.noarch ${status} = PASS ${status\_message} = None ${run\_cmd} = rpm -q java-11-openjdk rpm -q java-11-openjdk Running command 'rpm -q java-11-openjdk 2>&1'. ${output} = java-11-openjdk-11.0.20.0.8-3.el9.x86\_64 ${status} = PASS ${status\_message} = None ${run\_cmd} = rpm -q python3 rpm -q python3 Running command 'rpm -q python3 2>&1'. ${output} = python3-3.9.16-1.el9\_2.1.x86\_64 ${status} = PASS ${status\_message} = None ${run\_cmd} = rpm -q openssl rpm -q openssl Running command 'rpm -q openssl 2>&1'. ${output} = openssl-3.0.7-17.el9\_2.x86\_64 ${status} = PASS ${status\_message} = None ${run\_cmd} = rpm -q pam rpm -q pam Running command 'rpm -q pam 2>&1'. ${output} = pam-1.5.1-14.el9.x86\_64 ${status} = PASS ${status\_message} = None ${run\_cmd} = rpm -q python3-setuptools rpm -q python3-setuptools Running command 'rpm -q python3-setuptools 2>&1'. ${output} = python3-setuptools-53.0.0-12.el9.noarch ${status} = PASS ${status\_message} = None Length is 0 |

Table- Verify required utilities are available

|  |  |
| --- | --- |
| section | s1-s3 |
| Purpose | Cisco NSO requires some utilities, this test verfies these binaries exist |
| procedure |  |
| status | PASS |
| messages | ${command} = which ${check\_string} = /usr/bin/which: no ${errors\_list} = [] ${run\_cmd} = which tar which tar Running command 'which tar 2>&1'. ${output} = /usr/bin/tar ${status} = PASS ${status\_message} = None ${run\_cmd} = which gzip which gzip Running command 'which gzip 2>&1'. ${output} = /usr/bin/gzip ${status} = PASS ${status\_message} = None ${run\_cmd} = which find which find Running command 'which find 2>&1'. ${output} = /usr/bin/find ${status} = PASS ${status\_message} = None ${run\_cmd} = which ssh-keygen which ssh-keygen Running command 'which ssh-keygen 2>&1'. ${output} = /usr/bin/ssh-keygen ${status} = PASS ${status\_message} = None Length is 0 |

Table- Verify Hostname is not set to localhost

|  |  |
| --- | --- |
| section | s1-s3 |
| Purpose | Hostname Should not be localhost |
| procedure |  |
| status | PASS |
| messages | Running command 'hostnamectl hostname 2>&1'. ${output} = robot-dev-00 |

Table- Verify DNS servers are Configured

|  |  |
| --- | --- |
| section | s1-s3 |
| Purpose | DNS Servers should be Configured |
| procedure |  |
| status | PASS |
| messages | Running command 'more /etc/resolv.conf 2>&1'. ${output} = # Generated by NetworkManager search localdomain nameserver 192.168.1.1 nameserver 8.8.8.8 |

Table- Verify NTP servers are Configured

|  |  |
| --- | --- |
| section | s1-s3 |
| Purpose | NTP Servers should be Configured |
| procedure |  |
| status | PASS |
| messages | Running command 'chronyc sources 2>&1'. ${output} = MS Name/IP address Stratum Poll Reach LastRx Last sample =============================================================================== ^- ntp1.trans-ix.nl 2 10 ... |

Table- Verify NTP service is active

|  |  |
| --- | --- |
| section | s1-s3 |
| Purpose | Check that the NTP service is active |
| procedure |  |
| status | PASS |
| messages | Running command 'timedatectl show | grep -Po '(?<=NTPSynchronized=)[^,]+' 2>&1'. ${output} = yes |