

COMMON CRITERIA GUIDE

HYCU for Enterprise Clouds Administrative Guide

Document release date: December 2023



Legal notices

Legal notices

Copyright notice

© 2023 HYCU. All rights reserved.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, distributed, transmitted, stored in a retrieval system, modified or translated to another language in any form by any means, without the prior written consent of HYCU.

Trademarks

HYCU logos, names, trademarks and/or service marks and combinations thereof are the property of HYCU or its affiliates. Other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.

Acropolis and Nutanix are trademarks of Nutanix, Inc. in the United States and/or other jurisdictions.

Azure®, Microsoft®, Microsoft Edge™, and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

GCP™, Google Cloud Platform™, and Google Cloud Storage™ are trademarks of Google LLC.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Red Hat Enterprise Linux is a registered trademark of Red Hat, Inc. or its subsidiaries in the United States and other countries.

VMware ESXi™, VMware Tools™, VMware vCenter Server®, VMware vSphere®, VMware vSphere® Data Protection™, and VMware vSphere® Web Client are registered trademarks or trademarks of VMware, Inc. and its subsidiaries in the United States and other jurisdictions.

Disclaimer

The details and descriptions contained in this document are believed to have been accurate and up to date at the time the document was written. The information contained in this document is subject to change without notice.

HYCU provides this material "as is" and makes no warranty of any kind, expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. HYCU shall not be liable for errors and omissions contained herein. In no event shall HYCU be liable for any direct, indirect, consequential, punitive, special or incidental damages, including,

without limitation, damages for loss and profits, loss of anticipated savings, business interruption, or loss of information arising out of the use or inability to use this document, or any action taken based on the information contained herein, even if it has been advised of the possibility of such damages, whether based on warranty, contract, or any other legal theory.

The only warranties for HYCU products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty.

Notice

This document is provided in connection with HYCU products. HYCU may have copyright, patents, patent applications, trademark, or other intellectual property rights covering the subject matter of this document.

Except as expressly provided in any written license agreement from HYCU, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property on HYCU products. Use of underlying HYCU product(s) is governed by their respective Software License and Support Terms.

Important: Please read Software License and Support Terms before using the accompanying software product(s).

HYCU

www.hycu.com

Contents

Introduction	5
Evaluated configuration	5
Scope of the evaluation	5
Configuration	6
1. Deploying HYCU	6
2. Logging on to HYCU Remotely	6
3. Logging on to HYCU Locally	7
4. Admin Management	7
5. Enabling the CC-compliant mode	7
6. Cryptographic Requirements Enforced by the TOE in CC-mode	8
7. Performing the self-test	10
8. Configuring access banners	10
9. Configuring system time	11
10. Configuring SSL certificates	12
11. Using a TLS Server (Syslog, AD, SMTP)	14
12. Prerequisites	15
13. Configuring the sending of audit records to an external syslog server	15
14. TLS Server Requirements	16
15. System Behavior for Audit Logs	16
16. Auditable Events	17
17. NDcPP Audit Events	18
18. Passwords on HYCU	25
19. Configuring session timeouts	25
20. Upgrading the HYCU Appliance	26
21. Managing Certificate Revocation	27
22. Configuring failed login count and lock duration	27

Introduction

This document provides guidance on the configuration and operation of HYCU Data Protection for Enterprise Clouds (HYCU) for the purposes of the Common Criteria (CC) evaluation. It describes operations specific to the CC-compliant mode. This document supplements the *HYCU User Guide*.

HYCU for Enterprise Clouds allows administrators to protect and manage clusters of a virtualized infrastructure with one integrated interface.

TOE Physical acquisition

The testing laboratory received and accepted the Target of Evaluation (TOE) to the testing facility. TOE was delivered via commercial carrier, and it contained a packing slip that listed the serial number of the device (consistent with the guidance documentation).

Evaluated configuration

The Target of Evaluation (TOE) is HYCU 4.5.1, deployed as a virtual appliance on a VMware vSphere 7.0 hypervisor running on a Lenovo ThinkSystem SR630, Xeon Silver 4208. The following table describes the TOE environment:

Component	Description
Lenovo ThinkSystem SR630, Xeon Silver 4208	TOE Hardware platform
VMware ESXi 7.0	Hypervisor
VMware vCenter 7.0	Virtualization management
LDAP/S server	Remote authentication
SMTP/S server	Notifications
HTTPS Webhooks	Auditing server
DNS server	Name resolution
Administrator Workstation	Management of the TOE

For details, see the Security Target document.

Scope of the evaluation

The scope of the evaluation includes:

- HYCU operating in the HYCU Backup Controller mode
- Web UI operation including administrative and security configuration
- Text console operation including administrative and security configuration
- Use of LDAP/S for remote authentication
- Use of SMTP/S for e-mail notifications

- Use of HTTPS Webhooks for auditing

The scope of the evaluation does not include:

- SSH access
- Any backup target configuration
- Any backup and restore functionality
- Application awareness
- Mutually authenticated TLS
- Any use of NTP

Configuration

1. Deploying HYCU

For details, see the *HYCU User Guide*, Ch. 2 “Deploying the HYCU Virtual appliance”.

2. Logging on to HYCU Remotely

After you successfully deploy the HYCU virtual appliance, you can access HYCU by using a web browser.

Procedure

1. In a supported browser, enter the following URL:
 - a. `https://<serverName>:8443` In this instance, is the fully qualified domain name of the HYCU server.
 - i. For example: <https://hycu.example.com:8443>
 - b. On the logon page, depending on how you want to log on to HYCU, do one of the following:
 - i. By using dedicated logon credentials for HYCU. Enter your logon name and password. You can use the default user name (admin) and password (admin) for initial access to HYCU. For security purposes, it is highly recommended that you change the default password.
 - ii. By using an identity provider. Click the preferred identity provider, and then, if required, enter your credentials.
 - c. To logout of this interface, go to the top right drop-down and click “Sign Out”

3. Logging on to HYCU Locally

Some operations require text-based console access. To log on to the text-based console, follow these steps:

1. Log on to the VMware vCenter User Interface.
2. Access the text console window of the HYCU appliance.
3. Log on with the user **hycu** (default password: **hycu/4u**).
4. Log out of this interface with the command "logout"

Most administrative operations require elevated privileges obtained using sudo. No authentication data is revealed while entering authentication information on this interface. This interface lets the user know they are local by displaying the tty session number.

4. Admin Management

The TOE can be managed via the web GUI and local console. Management activities that can be performed through the web GUI include the following:

- Start and stop services
- Update the TOE
- Modify the behavior of the transmission of audit data to an external IT entity
- Ability to configure audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full)
- Manage the cryptographic keys
- Configure the cryptographic functionality
- Manage the TOE's trust store and designate X509.v3 certificates as trust anchors.
- Import/export/generate X.509v3 certificates to the TOE's trust store.

The following management activities can be performed using the console:

- Set the time which is used for time-stamps (console only)
- Configuring access banners
- Ability to configure the session inactivity time before session termination or locking.
- Ability to configure the authentication failure parameters

5. Enabling the CC-compliant mode

Ensure you are running the evaluated TOE version, by checking contents of file /opt/grizzly/VERSION match the following:

To manage the CC-compliant mode, log on to the text-based console and follow these steps:

1. To enable the CC-compliant mode, run the following commands:

```
sudo /opt/grizzly/bin/enable_cc.sh --enable
sudo reboot
```

2. To disable the CC-compliant mode, run the following commands:

```
sudo /opt/grizzly/bin/enable_cc.sh --disable
sudo reboot
```

3. To view status of CC-compliance, run the following command:

```
sudo /opt/grizzly/bin/enable_cc.sh -status
```

i Important CC-compliant mode settings do not persist across upgrades. After you upgrade HYCU, you must manually re-enable the CC-compliant mode.

Setting the TOE into CC-Compliant mode restricts the device to the following cryptographic protocols and algorithms. The generation, importing, and deletion of cryptographic keys is restricted to the security administrator. RNG is configured automatically and appropriately initialized on TOE start.

6. Cryptographic Requirements Enforced by the TOE in CC-mode

TLS Ciphers when used in HTTPS, Syslog, SMTP and AD-TLS connections:

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289

The following ECC curves are supported by the device and no other curves are allowed or enabled:

- secp256r1
- secp384r1
- secp521r1

The following Cryptographic Hash algorithms are supported by the TOE:

- SHA-1
- SHA-256
- SHA-384

The following message digest sizes are supported by the TOE:

- 160
- 256
- 384

The following RSA key sizes are supported by the TOE:

- 2048
- 3072
- 4096

The TOE uses keyed-hash message authentication supporting TLS and HTTPS. TLS and HTTPS use the following:

- HMAC-SHA-1
 - Block size – 64 bytes
- HMAC-SHA-256
 - Block size – 128 bytes
- HMAC-SHA-384
 - Block size – 128 bytes

NOTE: There is no provisioning supported besides enabling CC-Mode. For all the servers that use TLS, the Admin provisions the server information, and the TOE creates the TLS connection to the server. When a connection is severed then the TOE will detect that state and will automatically re-connect and perform retry attempts as needed. The administrator does not need to perform any actions. This applies to SMTP, LDAP/S, and Syslog. If the IT entity server is non-functional then that equipment and application will need to be recovered.

7. Performing the self-test

HYCU has a built-in self-test to ensure the integrity of critical files on the appliance.

In the CC-compliant mode, the self-test is executed on HYCU startup and reload, and the results are audited.

To perform the self-test manually, log on to the text-based console and run the following command:

```
sudo /opt/grizzly/bin/hycu-selftest.sh
```

Possible errors during self-test are:

- Checksum database file is missing or corrupted.
- One or more files from the checksum database are missing on the TOE.
- One or more files from the checksum database do not match their checksum on disk.

Any of these situations indicate a corrupted or compromised state of the TOE. The only response is for TOE to be reinstalled or reset. For example, OS image should be replaced with the fresh image state, while retaining the existing data disk.

Self-tests are run before the server is started ensuring that the state of the application server and cryptographically relevant parts of the OS have not been tampered with and match the state at release time.

As mandated by FIPS-140-2, self-test is performed on cryptographic library initialization at first operation involving the cryptographic library.

If this self-test passes, operations continue normally.

If this self-test fails, the self-test failure reason is logged, and TOE startup is prevented.

The native cryptographic library (OpenSSL) self-test failure prevents Apache httpd startup.

Java cryptographic library (BouncyCastle) self-test failure prevents HYCU application (grizzly) startup.

Example Logs of Failed Self-Tests:

2023-12-14T11:10:21.902287+00:00 polaris13 info daemon httpd 3169242 - crypto/fips/fips.c:154: OpenSSL internal error: FATAL FIPS SELFTEST FAILURE

2023-12-14T11:32:11.310230+00:00 polaris13 info daemon grizzly.sh 3171945 - Exception in thread "main" org.bouncycastle.crypto.fips.FipsOperationError: Module checksum failed: SHA-256 digest error for META-INF/HMAC.SHA256

8. Configuring access banners

To configure access banners, follow these steps:

1. Log on to the text-based console.
2. Make the following files available in `/hycudata/var/branding`:

File name	Format	Purpose
<code>loginImage.*</code>	PNG, JPG	Login screen background (1574×1920)
<code>loginLogo.*</code>	PNG, JPG	Logo on login screen (140x20)
<code>pageLogo.*</code>	PNG, JPG	Logo on expanded menu (140x20)
<code>pageSmallLogo.*</code>	PNG, JPG	Logo on collapsed menu (50x20)
<code>loginTitle.txt</code>	Text – single line	Main title on login screen
<code>loginSubtitle.txt</code>	Text – single line	Subtitle on login screen
<code>console.txt</code>	Text	Pre-login banner for SSH/text-based console

3. Update the branding configuration by running the following command:

```
sudo /opt/grizzly/bin/hycu-branding.sh
```

i Important You may need to force refresh the HYCU UI in the browser for the changes to take effect.

9. Configuring system time

NTP time synchronization is disabled in the CC-compliant mode.

To configure system time, follow these steps:

1. Log on to the text-based console.
2. Modify the system time by running the following command:

```
timedatectl set-time "YYYY-MM-DD HH:MM:SS"
```

10. Configuring SSL certificates

To establish trusted and secure communication in your data protection environment, you must configure SSL certificates.

To access the SSL Certificates dialog box, click **Administration**, and then select **SSL Certificates**.

Generate a certificate signing request:

1. Click **Generate**, then **Generate certificate signing request**.
2. Enter the name of the certificate signing request in the **Name** field.
3. Verify the name in the **Common Name** field.
4. Enter the organization name in the **Organization** field.
5. Enter the organization unit in the **Organization Unit** field.
6. Enter the location in the **Location** field.
7. Select the proper country from the **Country** field.
8. Select the Key Algorithm from the **Key Algorithm** selection box.
9. Select the key size from the **Key Size** selection box.
10. Click Generate.

Importing a custom certificate:

Prerequisites

- The certificate is compliant with the PKCS#7 standard and encoded in the PEM format.
- All certificate files are unencrypted.
- For importing an SSL key pair:* The private key and the certificate are available
- For importing a CA-signed certificate:* The CA-signed certificate or trust chain certificates are available.

Procedure

1. In the SSL Certificates dialog box, click **Import**. The Import dialog box appears.
2. Depending on whether you want to import an SSL key pair or a CA-signed certificate, click one of the following tabs and follow the instructions:

Tab	Instructions
SSL keypair	<p>a. Enter a name for your certificate.</p> <p>b. Browse for the following files:</p> <ul style="list-style-type: none"> • <i>Optional.</i> CA certificate/chain: The file with the CA-signed certificate or trust chain certificates. • Certificate: The file with the certificate corresponding to the private key that you are importing. • Private key: The file with the private key that is associated with the certificate that you are importing. <p>The private key should be created with the RSA or ECDSA algorithm in the PKCS#1 or PKCS#8 format. The minimum key size for private keys created with the RSA algorithm is 2048 bits.</p>
CA certificate/chain	<p>a. Enter a name for your certificate.</p> <p>b. Browse for the file with the CA-signed certificate or trust chain certificates.</p>

3. Click **Import**.

You can also change the name of any self-signed or custom certificate (click **Edit** and make the required modification) or delete the ones that you do not need anymore (click **Delete**).

Deleting an SSL certificate:

1. Select the certificate in the SSL certificates box.
2. Click the Delete button.
3. Click Yes in the dialog box asking "Are you sure you want to remove the certificate: <Certificate Name>?"

For more details, see the *HYCU User Guide*, Ch. 11 "Administering", section "Configuring SSL certificates", which contains information about the following operations:

- Managing Certificate Signing Requests (CSR)
- Common Name
- Organization
- Organizational Unit

- Country
- Private key and certificate import and generation
- Configuration of trusted roots with a CA
- Configuring the HTTPS server certificate

Note: Only an administrator has the ability to configure any of the above. Public keys, private keys and passwords are stored in the PostgreSQL database and are deleted using DELETE SQL statement. On-disk data is garbage-collected and legible for overwrite after autovacuum daemon executes the VACUUM SQL statement if there is a delay or prevention on key destruction. No configuration is required for the operating environment so the TOE can use certificates.

11. Using a TLS Server (Syslog, AD, SMTP)

Use the following to configure an audit server:

Refer to section 13 “Configuring the sending of audit records to an external syslog server”.

Use the following to configure an AD server:

1. Click Settings, click identity providers, then click **+New**.
2. Type the name for the Authentication account.
3. Verify in the **Type** field it says, **Active Directory**.
4. In the **Domain** field type the domain of the authentication server.
5. In the **Provider URL** field type the IP address of the provider URL, it would be in the format of ldap(s)://<Domain Controller Hostname/IP>:[<port>].
6. Click Save

Note: To stop the above service, delete the setting that have been configured.

Use the following to configure an SMTP server:

1. Click Settings, then click **SMTP server settings**.
2. In the **Display name** field type the name of the SMTP server account.
3. The **Hostname or IP Address** field type in the hostname of the SMTP server.
4. Verify in the **port** field that it states 25.
5. Verify in the **Security Mode** it says “STARTTLS”.
6. In the **From Email Address** field type the email address that will show up that the appliance will send emails from.

Note: To stop the above service, delete the setting that have been configured.

12. Prerequisites

- You must be logged in to HYCU using an account with at least admin access privileges.
- You have the server host name and filename for the X.509 certificate files.
- Device certificate with private key and CA certificate has been installed on the TLS server.
- You know the host name for the TLS server.
- The reference identifier is configured in the POST URL in the webhook notifications field.

Note: A security administrator can enable communication to an external audit server via TLS. A security administrator can also disable audit log sending by clearing the notification configuration. There is no provision for disabling any of the other services. The administrator is also able to start services such as the authentication and SMTP server via TLS. If a connection becomes unintentionally broken, the TOE will reattempt to connect until communication is restored securely. If the admin wants to stop any of the services mentioned above, they will have to remove the reference to the TLS server used by the TOE (Syslog, AD/s, SMTP/s).

13. Configuring the sending of audit records to an external syslog server

HYCU uses HTTPS POST webhooks to send audit data over a secure channel.

Procedure:

1. In the Notifications dialog box, click the **Webhooks** tab, and then click **+ New**.
2. Enter a name for the webhook notification and, optionally, its description.
3. From the Category drop-down menu, select one or more categories to which the events belong (for example, Policies, Backup, Credentials, System, and so on). To include all categories, click **Select All**.
4. From the Status drop-down menu, select the status of the events (Success, Warning, Failed). To include all statuses, click **Select All**.
5. From the Language drop-down menu, select the preferred language for webhook notifications.
6. In the Post URL field, enter the URL of the endpoint the webhook notifications should be sent to in one of the following formats:
 - a. <https://<host>>
 - b. <https://<host>/<Path>>
7. Click **Next**.
8. Click **Save**.

To disable HYCU audit log service.

Procedure:

1. In the Notifications dialog box, click the Webhooks tab.
2. Click the most recent addition in the Webhooks tab, highlighting your selection.
3. Click the delete button just above your selection.
4. Click "Yes" in the dialog box stating, "Are you sure you want to remove webhook notification setting <Webhook name>?"

For more details, see the *HYCU User Guide*, Ch. 9 "Performing daily tasks", section "Setting up webhook notifications".

i Important Make sure that you are using an HTTPS webhook URL, and that you can establish trust with the webhook server (for example, by importing an appropriate trusted root).

14. TLS Server Requirements

The TLS server must be a server that supports TCP and TLS v1.2. This is supported by default and can't be configured by an administrator. The presented reference identifier conforms to RFC 6125 section 6 where the CN or SAN of the certificate must match the hostname configured on the TOE.

15. System Behavior for Audit Logs

The TOE can be configured to export audit events securely to a syslog server using TLS v1.2 protocol using X.509 certificates. No configuration is necessary to enforce TLSv1.2 connection due to the device denying connections from clients requesting any lower SSL versions.

Audit events are stored locally and are also sent to an external audit server as they are created. TLS is used to provide a trusted communication channel with the audit server. Only a security administrator is allowed the ability to modify the behavior of transmitting audit data to a syslog server.

Audit data is stored locally in a Postgres database (database 'grizzly', table 'event'). There is no set limit on the local audit data storage, beyond data disk size. An administrator can configure the database to purge events older than a specified date.

Normally, the TOE sends audit records to the audit server as they occur. If communication with the audit server fails, events are stored locally and when the connection is restored all stored audit records will be transmitted to the remote audit server.

If local storage space is exhausted new audit records are dropped. Other than an administrator being able to clear the local audit records there is no provision to modify the records. An audit record is generated when the audit log is cleared.

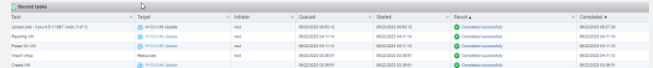
16. Auditable Events

The TOE generates a comprehensive set of audit logs that identify specific TOE operations whenever an auditable event occurs. Auditable events are specified in Table 1. Each audit record contains the date and time of event, type of event, subject identity, and the outcome (success or failure) of the event.

17. NDcPP Audit Events

Requirement	Auditable Events	Additional Audit Record Contents	Sample Audit Records
FAU_GEN.1	Start-up of the audit function	None	2023-09-20T18:40:00.332 INFO @000FD === Loading configuration from file /opt/grizzly/logs/logging.properties (com.comtrade.ntx.common.config.FileConfig load)
	Shutdown of the audit function	None	2023-09-21T15:20:13.061714+00:00 HYCU info daemon systemd 1 - Stopping Grizzly HTTP Server...
	Administrative Login	Name of user account shall be logged if individual user accounts are required for Administrator s	2023-09-20T18:19:16.637 INFO @00029 User 'admin' logged-in from IP address 192.168.254.230 (com.comtrade.ntx.restservice.security.TokenAuthentication setToken)
	Administrative Logout		2023-09-21T13:44:19+00:00 localhost info user grizzly - - HYCU Backup: User admin successfully logged out.
Changes to TSF data related to configuration changes	In addition to the information that a change occurred, it shall be logged what has been changed		body: {"severity":"INFO","created":"1695237054739","details":"Successfully added user testuser123 to group Infrastructure Group as Administrator.", "category":"USER_GROUPS","message":"Successfully added user to group.", "user":"Infrastructure Group", "taskId":"N/A"} failed with exception: java.lang.NullPointerException: NullPointerException invoking https://hycutest.com:5001/: null [0] (com.comtrade.ntx.restclient.RestClient post)
Generating/import of cryptographic keys	In addition to the action itself, a unique key name or key reference shall be logged		2023-09-20T19:12:35.702 INFO @00020 Reading CA chain, cert #1 (com.comtrade.ntx.model.schemas.cfgdb.Certificate buildCertificateChain) 2023-09-20T19:12:35.703 INFO @00020 cert #1, subject'CN=RootCA,ST=MD,C=US', expires: 'Sat Apr 13 18:32:00 UTC 2024', issuer: 'CN=RootCA,ST=MD,C=US' (com.comtrade.ntx.model.schemas.cfgdb.Certificate buildCertificateChain) 2023-09-20T19:12:35.815 INFO @00020 Successfully added certificate. (com.comtrade.ntx.restservice.customizations.RestCommons getResponse)
Changing of cryptographic keys			2023-09-21T15:12:50.599 INFO @00A2F storing 'CN=10.1.3.122,OU=NutanixTeam,O=HYCU,L=Ljubljana,ST=Slovenia,C=SI' to /etc/pki/tls/certs/hycussl-69762b97-cac7-4a69-9200-bddcd3a65a79.crt (com.comtrade.ntx.networking.SystemNetwork setupHttpd) 2023-09-21T15:12:50.602 FINE @00A2F Executing the command: /bin/sudo bash -c mv /tmp/hycussl-69762b97-cac7-4a69-9200-bddcd3a65a79.crt /etc/pki/tls/certs/hycussl-69762b97-cac7-4a69-9200-bddcd3a65a79.crt (com.comtrade.ntx.common.cmd.CommandExecutor executeCommand)
Deleting of cryptographic keys			body: {"severity":"INFO","created":"1695237207480","details":"Successfully deleted certificate testCA.", "category":"CONFIG","message":"Successfully deleted certificate.", "user":"Infrastructure Group", "taskId":"N/A"}

	Resetting passwords	Name of related user account shall be logged.	2023-09-20T19:18:35.598 INFO @0002D Updating user : good11 (com.comtrade.ntx.restservice.Users updateUser) 2023-09-20T19:18:35.716 INFO @0002D Successfully updated user good11. (com.comtrade.ntx.restservice.customizations.RestCommons getResponse)
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session	Reason for failure	**Refer to logs found in FCS_TLSS_EXT.1**
FCS_TLSC_EXT.1	Failure to establish a TLS Session	Reason for failure	Failure to establish TLSC connection: 2023-09-20T17:09:57.739 INFO @000D6 Client raised fatal(2) certificate_unknown(46) alert: Failed to read record (org.bouncycastle.jsse.provider.ProvTlsClient notifyAlertRaised)
FCS_TLSS_EXT.1	Failure to establish a TLS Session	Reason for failure	Failure to establish TLSS connection: 2023-09-21T13:41:05+00:00 localhost info user grizzly - - HYCU Backup: httpd - from: 10.1.3.169:37224, to: 10.1.3.122:8443 - AH02008: SSL library error 1 in handshake (server HYCU:8443) 2023-09-21T13:41:05+00:00 localhost info user grizzly - - HYCU Backup: httpd - SSL Library Error: error:14209102:SSL routines:tls_early_post_process_client_hello:unsupported protocol
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g. IP address).	Unsuccessful login limit met: 2023-09-21T14:01:34+00:00 localhost info user grizzly - - HYCU Backup: Login for username: testuser123, From IP: 192.168.254.230, Login status: FAILED 2023-09-21T13:54:21+00:00 localhost info user grizzly - - HYCU Backup: User testuser123 has been locked from 192.168.254.218 for 15 minutes.
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).	Login Remote: 2023-09-20T18:19:16.637 INFO @00029 User 'admin' logged-in from IP address 192.168.254.230 (com.comtrade.ntx.restservice.security.TokenAuthentication setToken) Login Local: 2023-04-17T17:18:15.818498+00:00 null info authpriv login 301647 - LOGIN ON tty1 BY hycu
FIA_UAU_EXT.2	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).	**Refer to logs found in FIA_UIA_EXT.1**

<p>FIA_X509_EXT.1/Rev</p>	<p>Unsuccessful attempt to validate a certificate</p> <p>Any addition, replacement or removal of trust anchors in the TOE's trust store</p>	<p>Reason for failure of certificate validation</p> <p>Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store</p>	<p>Certificate validation failure: **Refer to logs found in FCS_TLSC_EXT.1**</p> <p>Management of Trust Store: **Refer to logs found in FAU_GEN.1 of this table where generating/import of cryptographic keys, Changing of cryptographic keys, and Deleting of cryptographic keys is found**</p>
<p>FMT_MOF.1/Manual Update</p>	<p>Any attempt to initiate a manual update</p>	<p>None.</p>	<p>Software update failure:</p>  <p>**Due to the TOE being virtualized, the upgrade logs would occur on the host esxi machine**</p>
<p>FMT_SMF.1</p>	<p>All management activities of TSF data.</p>	<p>None.</p>	<p>Ability to start and stop services: 2023-09-20T18:17:13.847 FINE @000D5 Reloading XiNotificationSettings for Xi handler... (com.comtrade.ntx.eventhandling.XiEventHandler reloadCfg)</p> <p>Ability to configure audit behaviour: 2023-09-20T18:17:13.819 INFO @0001F Deleting webhook 5d9e67c9-23e8-4b79-a120-c98bfb29ce24 (com.comtrade.ntx.restservice.Webhooks deleteWebhook)</p> <p>Ability to modify the behaviour of the transmission of audit data to an external IT entity: 2023-09-20T18:17:13.841 INFO @0001F Successfully deleted webhook. (com.comtrade.ntx.restservice.customizations.RestCommons getResponse)</p> <p>Ability to set the time which is used for timestamps: **Refer to logs found in FPT_STM.1**</p> <p>Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors: **Refer to logs found in FAU_GEN.1**</p> <p>Ability to manage the cryptographic keys: **Refer to logs found in FAU_GEN.1**</p>

Ability to import X.509v3 certificates to the TOE's trust store:

****Refer to logs found in FAU_GEN.1****

Ability to administer the TOE locally and remotely:

****Refer to logs found in FIA_UIA_EXT.1****

Ability to configure the access banner:

2023-02-09T19:55:28+00:00 localhost info user grizzly - - HYCU
Backup: sudo - hycu : TTY=tty1 ; PWD=/hycudata/var ; USER=root ;
COMMAND=/bin/mv console.txt loginImage.png sshd.txt
/hycudata/var/branding/

2023-02-09T19:58:30+00:00 localhost info user grizzly - - HYCU
Backup: sudo - hycu : TTY=tty1 ; PWD=/hycudata/var ; USER=root ;
COMMAND=/opt/grizzly/bin/hycu-branding.sh

Ability to configure the session inactivity time before session termination or locking:

2023-09-21T15:26:22+00:00 localhost info user grizzly - - HYCU
Backup: sudo - hycu : TTY=pts/1 ; PWD=/var/log ; USER=root ;
COMMAND=/bin/nano /opt/grizzly/config.properties

Ability to update the TOE, and to verify the updates using [hash comparison] capability prior to installing those updates:

****Refer to the logs found in FPT_TUD_EXT.1****

Ability to configure the authentication failure parameters for FIA_AFL.1:

2023-09-21T13:59:29.646469+00:00 HYCU info daemon grizzly.sh
38119 - PROPERTY: login.lock.interval.minutes=15
2023-09-21T13:59:29.647865+00:00 HYCU info daemon grizzly.sh
38119 - PROPERTY: login.max.failed.count=3

Ability to configure cryptographic functionality:

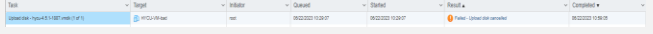
2023-12-06T23:20:56.422 FINE @00024 Starting to insert CSR data.

(com.comtrade.ntx.model.schemas.cfgdb.Certificate insertCsr)

2023-12-06T23:20:56.481 FINE @00024 Successfully inserted CSR data.

(com.comtrade.ntx.model.schemas.cfgdb.Certificate insertCsr)

2023-12-06T23:20:56.544 INFO @00024 Successfully generated Certificate Signing Request.

			(com.comtrade.ntx.restservice.customizations.RestComm ons getResponse)
FPT_STM.1	Discontinuous changes to time - either Admin actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See application note on FPT_STM_EXT .1)	For discontinuous changes to time. The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).	System Set time: 2023-09-21T14:13:45.000802+00:00 HYCU info daemon systemd-timedated 42012 - Changed local time to Thu Sep 21 14:13:45 2023 2023-09-21T14:14:15.041961+00:00 HYCU info daemon systemd 1 - systemd-timedated.service: Succeeded.
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None.	Software updates install failure:  **Due to the TOE being virtualized, the upgrade logs would occur on the host esxi machine** Successful software update:  **Due to the TOE being virtualized, the upgrade logs would occur on the host esxi machine**
FTA_SSL_EXT.1 (if “terminate the session” is selected)	The termination of a local session by the session locking mechanism.	None.	2023-09-21T14:33:02.579322+00:00 HYCU info auth systemd-logind 1281 - Removed session 12. 2023-09-21T14:33:02+00:00 localhost info user grizzly - - HYCU Backup: login - pam_unix(login:session): session closed for user hycu
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.	2023-09-21T14:27:31.223 INFO @00020 User token has expired atThu Sep 21 14:27:31 UTC 2023 (com.comtrade.ntx.restservice.security.TokenAuthentication isAuthorized)
FTA_SSL.4	The termination of an interactive session.	None.	2023-09-21T14:33:59+00:00 localhost info user grizzly - - HYCU Backup: User admin successfully logged out. 2023-09-21T14:33:59+00:00 localhost info user grizzly - - HYCU Backup: httpd - from: 192.168.254.230:58513, to: 10.1.3.122:8443 - AH02001: Connection closed to child 5 with standard shutdown (server HYCU:8443)

<p>FTP_ITC.1</p>	<p>Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.</p>	<p>Identification of the initiator and target of failed trusted channels establishment attempt.</p>	<p>Failed to establish connection to SYSLOG server: 2023-09-21T14:44:34.581 SEVE @000E0 Failed to send data to Webhook URL https://hycutest.com:5001. Error: NullPointerException invoking https://hycutest.com:5001: null (com.comtrade.ntx.eventhandling.WebhookEventHandler sendEventToWebhook)</p> <p>Failed to establish connection to AD/S server: 2023-09-21T14:40:43.550 FINE @0002C Using LDAPS for AD authentication (com.comtrade.ntx.restservice.security.ADAuthentication getADContext) 2023-09-21T14:41:13.677 WARN @0002C Invalid username or password specified or host not reachable (ldaps://10.1.5.40:636). 10.1.5.40:636 (com.comtrade.ntx.restservice.security.ADAuthentication getADContext)</p> <p>Failed to establish connection to SMTP/S server: 2023-09-21T14:42:42+00:00 localhost info user grizzly - - HYCU Backup: Failed to create smtp settings. 2023-09-21T14:42:42.541 WARN @00028 Failed to create smtp settings. (com.comtrade.ntx.restservice.customizations.RestCommons getResponse) 2023-09-21T14:42:42.541 WARN @00028 SMTP setting validation failed. Check the values you entered. Error: connect timed out (com.comtrade.ntx.restservice.customizations.RestCommons getResponse)</p>
<p>FTP_TRP.1/Admin</p>	<p>Initiation of trusted path. Termination of the trusted path. Failure of the trusted path functions.</p>	<p>None</p>	<p>Initiation of trusted path: body: {"severity":"INFO","created":"1695301643223","details":{"from: 192.168.254.230:60583, to: 10.1.3.122:8443 - AH01964: Connection to child 87 established (server HYCU:8443)","category":"SECURITY","message":"httpd - from: 192.168.254.230:60583, to: 10.1.3.122:8443 - AH01964: Connection to child 87 established (server HYCU:8443)","user":"sys","taskId":"N/A"}}</p> <p>Termination of trusted path: body: {"severity":"INFO","created":"1695301557115","details":{"from: 192.168.254.230:60534, to: 10.1.3.122:8443 - AH02001: Connection closed to child 83 with standard shutdown (server HYCU:8443)","category":"SECURITY","message":"httpd - from: 192.168.254.230:60534, to: 10.1.3.122:8443 - AH02001: Connection closed to child 83 with standard shutdown (server HYCU:8443)","user":"sys","taskId":"N/A"}}</p> <p>Failure of trusted path functions: **Refer to logs found in FCS_TLSS_EXT.1**</p>

Table 1

18. Passwords on HYCU

To configure the minimum password length for the HYCU UI, follow these steps:

1. Log on to the text-based console.
2. Add or modify the following line in the `/opt/grizzly/config.properties` configuration file:

```
user.password.min.length=<Length>
```

3. Reload the HYCU application by running the following command:

```
sudo systemctl reload grizzly
```

For details, see the *HYCU User Guide*, Appendix A “Customizing HYCU configuration settings”. The TOE supports passwords that can be composed of any combination of upper and lower case letters, numbers, and the following special characters: [“!”, “@”, “#”, “\$”, “%”, “^”, “&”, “*”, “(”, “)“]. Minimum password length is configurable to between [6] and [15] characters.

To configure the minimum password length for OS accounts, follow these steps:

1. Log on to the text-based console.
2. Add or modify the following line in the `/etc/security/pwquality.conf` configuration file:

```
minlen = <Length>
```

3. Create a new authselect configuration to enable password length enforcement for root account:

```
sudo authselect create-profile common-criteria -b $(authselect current -r)
```

4. Modify the following files:

- a. `/etc/authselect/custom/your-own-password-policy/system-auth`
- b. `/etc/authselect/custom/your-own-password-policy/password-auth`

In both files, replace the line starting with “password requisite “ with:

```
password requisite pam_pwquality.so local_users_only enforce_for_root
```

5. Apply the updated authselect profile:

```
authselect select custom/common-criteria
```

19. Configuring session timeouts

The session timeout mechanism applies to both the local and remote interfaces. To configure the session timeout for HYCU UI, follow these steps:

1. Log on to the text-based console
2. Add or modify the following line in the `/opt/grizzly/config.properties` configuration file:

```
api.session.expiration.minutes=<session timeout in minutes>
```

Default value is 15 (minutes).

3. Reload the HYCU application by running the following command:

```
sudo systemctl reload grizzly
```

To configure the session timeout for console sessions, follow these steps:

1. Log on to the text-based console
2. Modify the following line in the `/etc/profile.d/bash-logout.sh`

```
export TMOUT=<value in seconds>
```

Default value is 600 (10 minutes).

3. Log out and log on to the text-based console for changes to take effect.

20. Upgrading the HYCU Appliance

To upgrade the HYCU appliance, the administrator must obtain a legitimate update file from HYCU. The administrator can determine the current TOE version from either the console or web GUI and they can install a new version using the esxi web GUI after authentication as an administrator.

The TOE uses published hashes to determine the validity of the update file. Hash values can only be obtained from the HYCU website once the new update is provided. The security administrator is responsible for verifying the hash before performing any update functions. There is no hash verification done by the TOE, so it is the security administrators' responsibility to verify the hash is valid.

When an update is performed it takes effect immediately. None of the update procedures are automated. If the hash verification performed by the security administrator does not pass, the TOE shall not be updated. If the hash verification performed by the security administrator succeeds, the TOE can then be updated to the new version.

Once the update process is started, the TOE is completely unavailable to be managed or used until the update procedure is complete.

For more details, see the HYCU User Guide, Ch. 11 "Administering", section "Upgrading HYCU", which contains information about the upgrade functionality.

21. Managing Certificate Revocation

When configured in the CC-compliant mode, HYCU determines the revocation status as specified in RFC 6960 using OCSP. Certificate validation takes place on all TLS enabled connections (SMTP, syslog, LDAP/S). If a connection cannot be established for any of these TLS channels due to a failed validity check, the security administrator must ensure the certificate conforms to all requirements found in section 8.

To enable certificate revocation checking make sure you have the following line in the `/opt/grizzly/config.properties` configuration file:

```
cert.path.revocation.checking.enabled=true
```

i Important

After enabling/disabling the revocation checking, you need to reload the Hycu application running the command:

```
sudo systemctl reload grizzly
```

i Important If the TLS endpoint uses certificate revocation, the OCSP responder must be made available to HYCU, otherwise the certificate path validation will fail. Revocation checking takes place on all certificates in the presented chain. Bypassing this revocation policy is forbidden in the configuration for the TOE.

22. Configuring failed login count and lock duration

NOTE: The TOE will always allow an administrator to authenticate using the local console port, even if the account is locked. This behavior is not configurable.

To configure failed login count and lock duration, use the following steps:

1. Log on to the text-based console as an administrator.
2. Add or modify the following lines in the `/opt/grizzly/config.properties` configuration file:

```
login.max.failed.count=<max # of failed logins before lock (default: 3)>
```

```
login.lock.interval.minutes=<lock duration in minutes (default: 15)>
```

3. Reload the HYCU application by running the following command:

```
sudo systemctl reload grizzly
```



www.hycu.com

