IT Analytics Security and Encryption Reference

Release: 11.8

COHESITY

IT Analytics Security and Encryption Reference

Last updated: 2026-10-01

Legal Notice

Copyright © 2026 Cohesity, Inc. All rights reserved.

© 2026 Cohesity, Inc. All Rights Reserved. Cohesity, the Cohesity Logo and other Cohesity Marks are trademarks of Cohesity, Inc. in the US and/or internationally. The information supplied herein is the confidential and proprietary information of Cohesity and may only be used (a) by the intended recipients and (b) in conjunction with validly licensed Cohesity software and services. Find the terms of Cohesity licenses at www.cohesity.com/agreements.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. COHESITY SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Cohesity Support

Reach Cohesity Support

There are several ways to create a Cohesity support case.

- Go to Cohesity Support, to search in our knowledge base; or contact us by phone - United States and Canada: 1-855-9CO-HESI (926-4374), option 2.
- Log in to the Cohesity Support Portal to create a new case.
- Click the (**?**) icon on the Cohesity UI and select Support Portal.

Support/Service Assistance

First, contact the Service Provider that you have contracted for service and support. If you work directly with Cohesity and have a product warranty/entitlement, repair pricing, or technical support-related question, see your options below:

- To find solutions to your product issues or for suggestions or best practices, visit the Cohesity Knowledge Base.
- Log in to the Cohesity Support Portal to create a new case.
- To monitor your open cases, log in to the portal and click the **Cases** tab on the home page. This page should have all the case statuses and updates. You can also view individual case status.

Cohesity Software Running on Partner Hardware

For Cohesity software running on qualified third-party hardware, the following support workflow applies:

1. The customer may contact Cohesity Support first if the issue cannot be determined as a hardware issue.

   Note: Cohesity cannot process hardware replacement requests for partner hardware.

2. Cohesity Support triages the issue. If it is a software issue, Cohesity Support continues to work on it.
3. If it is a hardware/firmware issue or is suspected to be a hardware/firmware issue, Cohesity provides information about the issue to the customer and requests that the customer open a support ticket with the appropriate partner.
4. If needed, Cohesity Support can join a three-way call with the partner and the customer.
5. The customer informs Cohesity Support on the progress of the partner's case.

Contents

Chapter 1 IT Analytics Components and Security Compliance 5

Overview 5
Components of IT Analytics 5
Compliance with US Federal Government standards 6

Chapter 2 User Identity and Access Management 7

Overview 7
About user types 7
User groups 9
Domains 9
User authentication via single sign-on (SSO) 10
AD/LDAP Configuration 11

Chapter 3 Data Security and Encryption 17

Data Collector security and data encryption 17
Set up FIPS compliant Data Collector for File Analytics 18
Database security 18
IT Analytics data security at rest 19
Database connection properties 19
Modify the Oracle database user passwords 20
Encryption in subsystem communication with Data Collectors 21
Report security 25

Appendix A FAQs 27

Frequently asked questions and solutions 27

Chapter 1

IT Analytics Components and Security Compliance

This chapter includes the following topics:

- Overview
- Components of IT Analytics
- Compliance with US Federal Government standards

Overview

This document describes the various security standards and data encryption methods adhered to by Cohesity IT Analytics. Since the product has to probe several infrastructure nodes and data points to collect data, it adheres to strict security standards and encryption guidelines at various stages of data collection, storage, and processing. In addition, this document also talks about the in-house security standards and practices followed during patching of product issues and development of new features.

Components of IT Analytics

IT Analytics comprises of the following components:

1. Portal server: The physical server on which the NetBackup IT Analytics Portal server software is installed
2. Portal server software: The binaries, SQL, scripts, configuration files, and open-source or third-party software products needed to retrieve and render reporting data from the reporting database.

3. Reporting database: The Oracle database that stores all the report data. It is usually installed on the portal server but if required, can be installed on a separate dedicated database server. These binaries are installed during the first step of the installation procedure.
4. Data Collectors: The software that collects report data about your backup servers and storage arrays. The Data Collectors are usually installed on a separate server.

Compliance with US Federal Government standards

IT Analytics is compliant with the following United States Federal Government standards:

- Encryption: IT Analytics uses a FIPS 140-2 cryptographic library for at-rest encryption and in-flight encryption. However, full support for FIPS 140-2 is not enabled.
- Communication and data transfer: IT Analytics complies with both IPv4 and IPv6 for transferring data securely over the public and private networks. SSL/TLS protocols are followed for communication between networked systems. TLS 1.2 and TLS 1.3 are supported.
- Network security: IT Analytics adheres to Public key infrastructure (PKI) and 2-factor authentication for network security. Network can be configured to require Single Sign-on (SSO) in such a way that the PKI or 2-Factor Authentication of the SSO is inherited by IT Analytics.
- On Linux, IT Analytics is supported on RHEL which is configured to be STIG compliant. Apache, Oracle, and Tomcat subsystems of the product are STIG compliant. Application security and development requirements are met for all category-1 items as well as some category-2 and -3 items.
- Security Technical Implementation Guide (STIG): IT Analytics is supported on STIG-compliant RHEL. Moreover, the Apache, Oracle, and Tomcat subsystems are STIG compliant. The application security and development requirements adhere to CAT 1 STIG compliance level.
- IT Analytics data security at rest: IT Analytics users who want to ensure their IT Analytics data stored in Oracle Database is encrypted at rest must use the Oracle feature Transparent Data Encryption (TDE). TDE is part of the Oracle Advanced Security. It is available as an additional licensed option for the Oracle Database Enterprise Edition.

Chapter 2

User Identity and Access Management

This chapter includes the following topics:

- Overview
- About user types
- User groups
- Domains
- User authentication via single sign-on (SSO)
- AD/LDAP Configuration

Overview

This section describes the user creation and the user's role-based access rights in IT Analytics. The section also describes the secure access methods supported for the product.

About user types

There are three types of portal users:

Table 2-1 User types

User Type	Rights
Administrator	Manage user accounts and set up host groups at or below the Administrator's assigned group. An Administrator can create both End User and Administrator accounts, but only within the Administrator's home group. In an MSP (Managed Services Provider) environment, each client has Administrator accounts that have access only to the client's domain and only the host groups within that domain. **Note:** Portal upgrades will automatically enable privileges for newly added reports and the display of the **Inventory** view including all objects, for all Administrators. Refer to the release notes for the list of reports and features introduced in a specific product release.
Super User	Privileges available to this user cannot be revised by any other user. A Super User can do the following over and above the rights of the Administrator user: ■ Access the entire Portal host group hierarchy from top to bottom regardless of the user's group assignment. ■ Manage Oracle tablespace. ■ Define and manage server backup cycles. ■ Create both End User and Administrator accounts for any group within the host group hierarchy. ■ Access all default and user-generated reports. ■ View **New** and **Updated** badging on system report templates when they are made available. ■ Impersonate a user profile.
End User	■ The features for which privileges have been granted by the Administrator. End Users can utilize their privileges at or below their assigned home group. ■ An End User can create only End User accounts within the user's own home group (domain).

User groups

User groups provide an efficient way of managing many users at once. Administrator can assign privileges to a group and they are propagated to the users in that group. For example, privileges can:

- Enable access to specific reports
- Enable access to functional areas
- Restrict access to specific pages of the portal

Domains

A Domain provides a way to “partition” the reporting database into separate, private realms. It is used primarily to implement security controls for multi-tenancy systems and it is a unique entity associated with the top level of your host group hierarchy. The domain name is supplied during the installation process and the Portal assigns it to the root folder.

The domain is used by the Data Collector for:

- Authentication: The master server record must exist in the host group hierarchy for the domain. (Veritas NetBackup only)
- Host Searches: The Data Collector searches the domain’s host group hierarchy checking for hosts associated with the backup data it is gathering. If no host is found, a new host is added to the root-level host group folder for the domain.

Enterprise environments will typically have only one domain. When you add (or delete) host groups or attributes, you do so globally for your domain and all the host groups in that domain. Unless you are a Managed Services Provider (MSP), you do not have to specify a domain when you add or delete host groups or attributes through the Portal.

Multiple domains

If you are a Managed Services Provider, you need the capability of managing multiple, independent hierarchies - one for each of your client companies. As an MSP, you will define a unique domain for each of your customers. When you add or delete attributes, you can do so for all domains or you can select specific domains to apply changes.

A domain is associated with a host group hierarchy and all newly discovered hosts are added to the root host group associated with the domain. Each MSP customer will have a separate domain with its own hierarchy.

Note: A host group can only serve as the root for one domain. For example, you could have a host group defined for Acme Corp and then create an Acme Domain that uses the host group as the root of its host group hierarchy. Once a domain is associated with a host group, this host group cannot become the root of any other domain.

User authentication via single sign-on (SSO)

IT Analytics supports Single Sign On (SSO) for a standard unified login. User authentication is performed through an external Identity Management Server allowing for an increased level of security for user passwords and identity details. Hence, Single Sign-on requires SSL-enabled IT Analytics Portal, an external Identity Provider (IDP), and an external LDAP directory.

Single sign-on (SSO) prerequisites

- IT AnalyticsPortal must be SSL enabled (https protocol) using SSL certificates with the following properties:
  - Signature algorithm name: SHA256 with RSA
  - Subject public key algorithm: 2048-bit RSA key
- An external Identity Provider (IDP) that supports SAML 2.0
- SSL certificate must be added to the Portal Keystore using the Keystore Utility (deployCert)

Set up external identity provider (IDP) server

For the IDP to communicate with the IT Analytics Portal, an LDAP directory is configured on the external server for user management. Certain attributes must be populated for each user will log in to the Portal. Users must also belong to at least one group.

Users and groups in the external LDAP directory

Set the following attributes for each user in the external LDAP directory. For each attribute, the properties **name** and **friendlyName** must be present and have values populated. These attributes must be exposed by both the external LDAP directory and the IDP server. The names of attributes are as follows:

- displayName: <first_name> <last_name> For example Jane Smith
- email: email address
- mobile: cell phone or mobile number
- telephoneNumber: work phone or home phone number

- sAMAccountName: the unique user name that is used as a login
- memberOf: List of group names to which the user belongs.

Note: The attribute `memberOf` requires customization for a Microsoft Azure IDP. It is recommended to set **Groups Assigned to the application** instead of **All groups** or **Security groups** for "memberOf" attribute. Click here for more details.

Before using SSO to log into the Portal, an external user must belong to one external directory group that also exists as a User Group in the IT Analytics Portal. If the setup criteria is met, when the user logs into the Portal for the first time, the user's profile is synchronized from the external directory. The user also inherits all privileges assigned to the User Group.

Registration with the IDP server

The registration process occurs by exchanging metadata XML files between the IT Analytics Portal and the IDP server. On the Portal side, once SSO is configured and the Portal Tomcat service restarted, you can download the metadata XML file and provide it to the IDP server. This file contains the SSL certificate and identifies the IT Analytics as a service provider for SSO. A similar metadata XML file must be downloaded from the IDP server and provided to the Portal.

See the *Configure single sign-on (SSO) using security assertion markup language (SAML)* in *IT Analytics System Administration* guide.

AD/LDAP Configuration

IT Analytics supports user authentication and optionally supports authorization using Active Directory (AD) or Lightweight Directory Access Protocol (LDAP).

Configuration of AD/LDAP authentication and authorization is driven through the configuration parameters in `portal.properties` file.

AD/LDAP configuration properties

AD/LDAP configuration supports following properties and can be set in the in `portal.properties` file.

OS specific `portal.properties` file location:

- Linux: `/opt/aptare/portalconf/portal.properties`
- Windows: `C:\opt\aptare\portalconf\portal.properties`

Table 2-2 AD/LDAP Configuration Properties

Property	Description
ldap.enabled	To enable LDAP, set this property to true. Supported Values: true | false
ldap.searchBase	■ Location from where the search will be performed to locate users in the authentication directory. ■ Often referred to as the Active Directory (AD) Search Base, this is the starting point in the Active Directory tree for searching for LDAP users. This search base, in LDAP distinguished name format, contains a fully qualified domain name. IT Analytics supports only one Search Base. Example: `dc=example,dc=company,dc=com`
ldap.url	■ Set to the host and port of your AD. Note that this URL value has a prefix **ldap:**. If using SSL, change the prefix to ldaps. ■ If you are using Active Directory for your external LDAP configuration, you may want to use the global catalog port of 3268 instead of port 389. ■ If using SSL, you may want to use the secure global catalog port of 3269 or 636 for standard LDAPs. Example : `ldap://example.company.com:389` OR `ldaps://example.company.com:636`

Table 2-2 AD/LDAP Configuration Properties *(continued)*

Property	Description
ldap.dn	■ Set to the ID of a user who has permission to search the SEARCHBASE. This user must be able to search all LDAP directory servers. ■ IT Analytics requires a user that has privileges to search under the Base DN (Distinguished Name) within the Active Directory structure. This must be an account that has administrative privileges, typically an Administrator. It can be the Administrator account that was created when Active Directory was installed, or it can be an account that was created, and either was given administrative privileges or was placed into a group with administrative privileges. ■ If you use Active Directory, specify this setting because Active Directory services do not allow anonymous binds. Microsoft Active Directory requires the username and password of a user that has enough privileges to search the LDAP directory. Example: `ldap.dn =CN=Admin,CN=Users,DC=example, DC=company,DC=com`
ldap.password	Set to the password of the user who is used in ldap.dn property. It will get empty and encrypted value will be set in `ldap.password.encrypted` property when you restart Portal Tomcat Service after configuring LDAP.
ldap.password.encrypted	It is set when you restart the Portal Tomcat service after configuring LDAP. It has encrypted value of the `ldap.password` property.
ldap.loginAttribute	The login attribute used for authentication. This is the attribute name in Active Directory that specifies the username, such as *uid* or *sAMAccountName*. Example: `ldap.loginAttribute=sAMAccountName`

Table 2-2 AD/LDAP Configuration Properties *(continued)*

Property	Description
ldap.authorization	If set to true, Portal authorizes the user against AD groups. At least one AD group of which the new user is member must be configured as a User Group in the Portal. **Note:** If the AD group is not mapped with the User Group in the Portal, then authentication fails during login with the error: “No user group mapping present for external LDAP user.” Supported Values: true | false
ldap.newUserDomain	Portal domain name where new user gets created. It is only used if `ldap.authorization` is set to true. To find domain name in portal, navigate to **Admin** > **Domains** > **Domain Name** Example: `ldap.newUserDomain=example.company.com`
ldap.keystore	If SSL support is enabled for LDAP, then it must have: ■ The keystore path location which contains AD certificates ■ The aptare:tomcat permission **Note:** If SSL is not enabled for LDAP, then this must be commented out.
ldap.keystore.password	Password for the keystore which is set in `ldap.keystore` property. It will get empty and encrypted value will be set in `ldap.keystore.password.encrypted` property when you restart the Portal Tomcat Service after configuring LDAP. **Note:** If SSL is not enabled for LDAP, then this must be commented out.

Table 2-2 AD/LDAP Configuration Properties *(continued)*

Property	Description
ldap.keystore.password.encrypted	It is set when you restart the Portal Tomcat service after configuring LDAP. It has encrypted value of the `ldap.keystore.password` property. **Note:** If SSL is not enabled for LDAP, then this must be commented out.
ldap.disable.user.attribute.name (Available from 11.0)	Its value is the AD attribute that indicates whether the user is active or inactive. During Portal authentication via AD, the REST API uses the AD attribute assigned to this property to check whether the user is still an active AD user. For example, if `ad.user.active` is the AD attribute that indicates whether a user is active or disabled, then `ad.user.active` must be assigned as the value of this property (`ldap.disable.user.attribute.name=ad.user.active`).
ldap.disable.user.attribute.value (Available from 11.0)	Its value must be same as that value of the AD attribute (specified in `ldap.disable.user.attribute.name`), which indicates the AD user is disabled. For example: If `ad.user.active` is the attribute for user status in AD, it may have several values such as `live`, `inactive`, `joined`, and so on. If the value `inactive` indicates the user is disabled in AD, then `inactive` must be set as value for this property (`ldap.disable.user.attribute.value=inactive`). REST API matches this value with the value of the AD attribute specified in `ldap.disable.user.attribute.name` property. If the values match, the user is disabled on the IT Analytics Portal. **Note:** A Portal super user must explicitly activate the user that was deactivated in both AD and Portal in the past but is again activated only in AD. A Portal administrator with adequate privilages can also activate such a user. Without user activation, Portal access will be restricted.

To configure AD/LDAP for user authentication as well as authorization, Portal Administrator must create at least one User Group in portal which is also present in AD/LDAP as a UserGroup.

LDAP support over SSL

If you are using a self-signed certificate or an AD certificate from a non-standard certificate authority (CA), you need a keystore having the AD certificate and update the LDAP configuration in the `portal.properties` file. You can skip this if you are using a standard certificate from a CA.

Chapter 3

Data Security and Encryption

This chapter includes the following topics:

- Data Collector security and data encryption
- Set up FIPS compliant Data Collector for File Analytics
- Database security
- Encryption in subsystem communication with Data Collectors
- Report security

Data Collector security and data encryption

Data collectors offer asymmetric encryption, also known as public-key cryptography. With this form of encryption, keys come in pairs - what a single key encrypts, only the other key can decrypt. This method of encryption provides additional security when data is collected.

In an upgrade scenario, you must enable asymmetric encryption for better security by generating a key file. You can also choose to continue with the symmetric encryption method but it will be less secure than the asymmetric encryption. Key file generation can occur at any time after an upgrade or if there is an issue such as data corruption or a key is lost.

To use this feature in either a new installation or an upgrade scenario, a key file must be manually generated in the Portal. When you add a data collector in the Portal, you download the key and then point to that location when you install the data collector software on the collector server. For existing data collectors, key generation for asymmetric encryption can occur at any time. You can opt-in to encrypt/decrypt credentials.

Set up FIPS compliant Data Collector for File Analytics

To become FIPS 140-2 compliant, you must configure the Data Collector for File Analytics as recommended below:

1. To enable FIPS compliance, you must install the Data Collector on a FIPS-compliant system.
2. Ensure that the Data Collector and the target Windows file server both are configured in FIPS mode.
3. Specify **vers=2** as the protocol version used between the collector and the target system.
4. Ensure Kerberos authentication is used on the target system.

Note: Steps to set up Windows file server in FIPS and Kerberos are beyond the scope of this document. You can refer the relevant product documentation for the same.

Database security

The Oracle database stores all report data. The Reporting Database is usually installed on the Portal Server, but you can just as easily install it on a separate server, preferably a dedicated database server. These binaries are installed during the first step of the installation procedure.

Data is managed in the Reporting Database with automatic purging scripts that run with specific retention periods per product and even data type. Some reports are more valuable when they have access to historical data. Because the Reporting Database only stores metadata, the amount of data on the Reporting Database is relatively small (GBs).

Oracle security profile for users

As recommended by Oracle, the ORA_STIG_PROFILE user profile is applied to all user accounts, unless a more restricted profile is used.

Some queries that retrieve more information on the user profiles are given below.

- To see which profile is used for PORTAL and APTARE_RO users and to view the properties of the resources under these profiles:

```
SELECT du.USERNAME, dp.PROFILE, du.ACCOUNT_STATUS, dp.*
FROM DBA_USERS du, DBA_PROFILES dp
```

```
WHERE du.username IN ('PORTAL', 'APTARE_RO')
AND du.profile = dp.profile
ORDER BY USERNAME;
```

- To view details of all the available user profiles that can be portentially used:

  ```
  SELECT * FROM DBA_PROFILES;
  ```

  To assign a profile to an existing user or to create a new profile, see Creating a Profile section of the Oracle documentation.

Note: : If any changes to the assignment of a user profile for PORTAL and/or APTARE_RO takes place then it may force to change the existing password of these users as per the new profile's restrictions. If the password for these users is then changed, it is mandatory to update in the application.

IT Analytics data security at rest

IT Analytics users who want to ensure their IT Analytics data stored in Oracle Database is encrypted at rest can explore Oracle feature Transparent Data Encryption (TDE). TDE is part of the Oracle Advanced Security. It is available as an additional licensed option for the Oracle Database Enterprise Edition.

TDE is transparent to business applications and does not require application changes. Encryption and decryption occur at the database storage level, with no impact to the SQL interface that applications use (neither inbound SQL statements, nor outbound SQL query results).

Oracle uses TDE to encrypt data at rest. In the event of storage media of Oracle Database data file being stolen, TDE helps protect the data stored on the media.

Database connection properties

The following table summarizes the portal.properties values for the Oracle users and passwords that are used by the portal.

Table 3-1 Portal properties with description.

Portal Property	Description
db.driver	This value is customized by the Portal installer and should not be modified.

Table 3-1 Portal properties with description. *(continued)*

Portal Property	Description
db.url	This is the address where the IT Analytics database resides. Depends on what was entered during the installation. This may need to be modified when there is a host name change.
db.user	The application DB user ID. Default value is portal and cannot be changed.
db.password db.password.encrypted=	Enter a password to be used with the DB user. The default value is **portal**. The password initially is stored in clear text, but after the restart of the Tomcat Portal services, the password is saved in the encrypted format and the clear text password is removed from portal.properties.
db.connection.max	Use this property to specify the maximum database connections allowed. The default value is 25.
db.connection.min	Use this property to specify the minimum number of database connections that the Portal can have. The default value is 25.
db.connection.expiration	When a Portal report initiates a long-running database query, this value (in minutes) establishes when the report will time out if the query takes too long to complete. The default value is 5.
db.ro_user_password db.ro_user_password.encrypted=	The Oracle database read-only user password for the IT Analytics database tables. The preset value is aptaresoftware123. The password initially is stored in clear text, but after the restart of the Tomcat Portal services, the password is saved in the encrypted format and the clear text password is removed from `portal.properties`.
db.sysdba_user	The Oracle database System DBA for the IT Analytics database tables. The preset value is system.

Modify the Oracle database user passwords

Use the following utilities to modify passwords for the Oracle database users **portal** and **aptare_ro**. These instructions apply only to user **portal** and **aptare_ro**.

- Linux: /opt/aptare/utils/changeDBPassword.sh
- Windows: C:\opt\aptare\utils\changeDBPassword.bat

The new password must not have the following characters:

- Double Quotes "".
- Back Slash '/'.
- Blank space ' '.

- Back Tick ‘`’

Note: If CyberArk feature is enabled, do not modify Oracle database password.

Complete these steps to modify passwords for the Oracle database user. These instructions apply to aptare_ro and portal users.

1. Login with root access on Linux or with admin access on Windows.
2. Stop the portal and agent Tomcat services.
3. Change the user password:

   On Linux:

   ```
   /opt/aptare/utils/changeDBPassword.sh -user <user_name> <password>
   ```

   On Windows:

   ```
   C:\opt\aptare\utils\changeDBPassword.bat -user <user_name>
   <password>
   ```

   This updates the specified user's password in Oracle configuration as well as the properties files like `portal.properties` and `datrarcvrproperties.xml`.
4. Restart the File Analytics services immediately after changing the password.

Encryption in subsystem communication with Data Collectors

Refer this table to check whether the Data Collector uses encrypted communication to talk to the target subsystem.

Module: Storage

Table 3-2 Communication with storage systems

Subsystem	Communication	Protocol	Port
Dell Compellent	Encrypted	SMI-S over https	5989
Dell EMC Elastic Cloud Storage (ECS)	Encrypted	https	4443
Dell EMC Unity	Encrypted	https	443, 8443

Table 3-2 Communication with storage systems *(continued)*

Subsystem	Communication	Protocol	Port
EMC data Domain Storage	Encrypted	ssh	22
EMC Isilon	Encrypted	ssh	22
EMC Symmetrix	FC based	-	-
EMC VNX (CLARiiON)	Encrypted	https	443
EMC VNX (Celerra)	Encrypted	https	443
EMC VPLEX	Encrypted	https	443
EMC XtremIO	Not encrypted	http	80
HP 3PAR	Encrypted	ssh	22
HP EVA	Encrypted	https	443
HPE Nimble Storage	Encrypted	https	configurable
Hitachi Block Storage	Not Encrypted	TCP	2001
Hitachi Content Platform (HCP)	Encrypted	https	9090
Hitachi NAS	Encrypted	ssc	206
Hitachi Vantara All-Flash and Hybrid Flash Storage	Encrypted	https	23451, 22016
IBM Cloud Object Storage	Encrypted	https	443
IBM Enterprise	Not Encrypted	TCP	1751, 1750, 1718
IBM SVC	Encrypted	ssh	22
IBM XIV	Encrypted	ssh	22
Microsoft Windows Server	Encrypted	WMI	NTLM/ Kerberos/ PktPrivacy

Table 3-2 Communication with storage systems *(continued)*

Subsystem	Communication	Protocol	Port
NetApp	Encrypted	https	443
NetApp Cluster-Mode	Encrypted	https	443
NetApp E-Series	Encrypted	SMCli	-
Pure Storage FlashArray	Encrypted	https	443
Veritas NetBackup Appliance	Encrypted	WMI Proxy	-

Module: Network and Fabrics

Table 3-3 Communication with network systems

Subsystem	Communication	Protocol	Port
Brocade Switch	Encrypted	https	443 (configurable)
Brocade Zone Alias	Encrypted	https	443 (configurable)
Cisco Switch	Encrypted	https	5989
Cisco Zone Alias	Encrypted	https	5989

Module: Virtualization

Table 3-4 Communication with virtualization technologies

Subsystem	Communication	Protocol	Port
IBM VIO	Encrypted	ssh telnet	22 23
Microsoft Hyper-V	Encrypted	WMI	NTLM/ Kerberos/ PktPrivacy
VMware	Encrypted	https	443

Module: File Analytics

Table 3-5 Communication with file management systems

Subsystem	Communication	Protocol	Port
File Analytics	Encrypted	NTLM	443

Module: Replication

Table 3-6 Communication with replication systems

Subsystem	Communication	Protocol	Port
NetApp	Encrypted	https	137 and 139

Module: Cloud

Table 3-7 Communication with cloud technologies

Subsystem	Communication	Protocol	Port
Amazon Web Services	Encrypted	https	443
Microsoft Azure	Encrypted	https	443
OpenStack Ceilometer	Encrypted	https	35357
OpenStack Swift	Encrypted	https	35357 (admin port) 5000 (Default public port)

Module: Data Protection

Table 3-8 Communication with data protection technologies

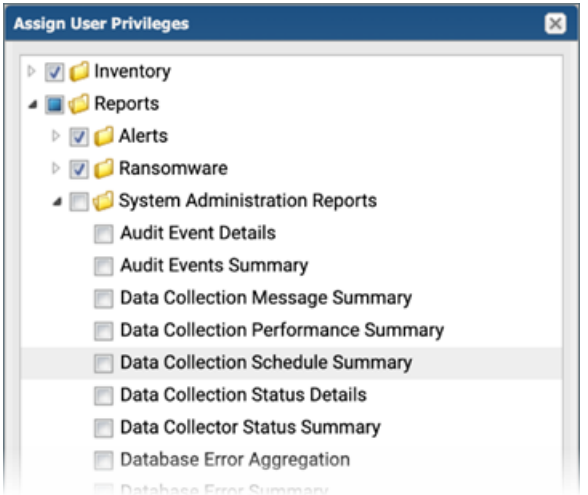
Subsystem	Communication	Protocol	Port
Cohesity DataProtect	Encrypted	https	443
Commvault Simpana	Encrypted	WMI Proxy	-
Dell EMC NetWorker Backup & Recovery	Encrypted	https	9090

Table 3-8 Communication with data protection technologies *(continued)*

Subsystem	Communication	Protocol	Port
EMC Avamar	Encrypted	ssh	22
EMC Data Domain Backup	ssh	ssh	22
EMC NetWorker	ssh	ssh	22
HP Data Protector	ssh	ssh	22
IBM Spectrum Protect (TSM)	Not Encrypted	TCP	1500
IBM Spectrum Protect Plus	Encrypted	https	443
NAKIVO Backup & Replication	Encrypted	https	443
Oracle Recovery Manager (RMAN)	Not Encrypted	jdbc	1521
Rubrik Cloud Data Management	Encrypted	https	443
Veeam Backup & Replication	Encrypted	wmi	NTLM/ Kerberos/ PktPrivacy
Veritas NetBackup	Configurable	ssh	22

Report security

System Administration reports in IT Analytics allow administrators to view information about the entire IT Analytics system. To ensure proper security, administrators must prevent non-administrators from having access to those reports. When setting up or modifying users in the **Admin** > **Users and Privileges** screen, disable **System Administration Reports** in the **Assign User Privileges** dialog:


Assign User Privileges
Inventory
Reports
Alerts
Ransomware
System Administration Reports
Audit Event Details
Audit Events Summary
Data Collection Message Summary
Data Collection Performance Summary
Data Collection Schedule Summary
Data Collection Status Details
Data Collector Status Summary
Database Error Aggregation

Appendix A

FAQs

This appendix includes the following topics:

- Frequently asked questions and solutions

Frequently asked questions and solutions

Q: How are passwords encrypted and which cryptographic algorithm is used for encryption?

A: If SSO integration is used to access the portal, user passwords are stored in the external SSO IdP. Otherwise, passwords are stored in Oracle encrypted AES128.

Q: What are the idle and absolute session timeout values?

A: Default idle session timeout is 15 days, but can be customized by the administrator.

Q: How is the user session managed?

A: A user session is managed using cookies.

Q: How is the Oracle DB password encrypted in the flat files? Is there any data in transit encrypted?

A: If Oracle and portal are installed on separate servers, the administrator can configure that connection to use TLS to encrypt that connection. When Oracle and portal are installed on the same server, the data is not encrypted between the Portal and Oracle.