Data Insight Feature Briefing

Box Cloud Storage Support

This document is about the new Box Cloud Storage Support feature in Symantec Data Insight 5.0.

If you have any feedback or questions about this document please email them to IIG-TFE@symatec.com stating the document title.

VERITAS™

Feature Description

Symantec Data Insight (DI) 5.0 now includes support for Box Cloud Storage. DI monitors the data stored on Box to provide access, ownership and permissions information.

DI will scan Box accounts on a scheduled basis or on an ad-hoc basis as needed. DI will be able to provide protection on sensitive data and provide management of data stored on Box.

Business Value

Adding support for Box further expands DI's capabilities. Customers can now gather important information on Box files such as data ownership, data access, and auditing as well as provide remediation workflow support.

Since its inception, DI continues to add support for various storage platforms. Monitoring files from Box enhances the benefits of DI by improving its intelligence of Box's cloud storage. This allows DI administrators to gain insight into access and ownership information of files stored on Box.

Monitor Box files with DI to:

- Discover unstructured Box file data using metadata, age, usage, and ownership to inform data lifecycle management, compliance and risk reduction initiatives
- Identify data owners and engage through a Self-service Portal to facilitate access control, data management and information security remediation efforts
- Enhance information protection with Symantec Data Loss Prevention integration

Underlying Principles

Box uses the Open Authorization 2 (OAuth2) protocol to permit DI access. DI leverages the Box Enterprise administrator credentials to gain access to the Box administrator account. This allows DI to gather information about all configured users and the activities each has performed. The administrator credentials authorize DI to access the Box Enterprise account. The authorization received from Box is saved as a named credential in the DI configuration.

With the integration of Box, Data Insight's capabilities remain generally the same, with a few differences for Box storage:

- Permissions Reporting continues to function for non-cloud-based file shares. For cloud shares, DI cannot obtain detailed information of the permission assigned to various users, files and folders.
- Entitlement Review Reports provide information as to who has permissions on a folder or file in Box. Although the report summarizes entitlements, the Self-service Portal does not allow users to perform any entitlement activities on Box shares.
- The only portal activity allowed on Box shares is for incident remediation. Incident remediation actions remain the same.

Prerequisites

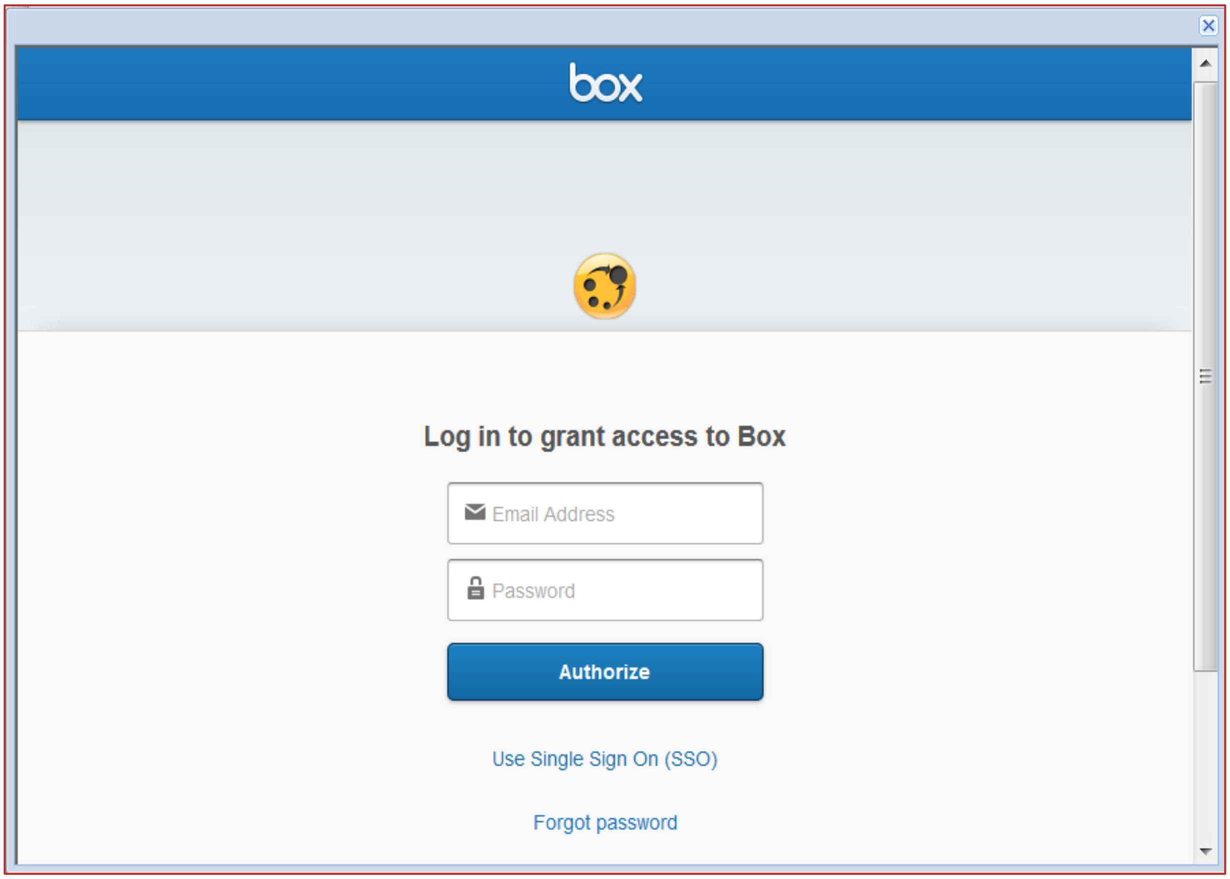
To monitor files located on Box, DI requires the following prerequisites are met:

- The organization must have:
  - An Enterprise Box account
  - Valid Box Enterprise administrator credentials to synchronize Box and DI (Box co-admin credentials are not sufficient)
- Ensure Box accounts are provisioned using Active Directory identities
- Data Insight must be installed and configured

Configuration

During the configuration process, the DI administrator configures Box settings in the DI interface in the **Settings** > **Cloud Services** section. The DI administrator identifies the **Collector** and **Indexer** worker nodes used for collecting and indexing the Box data. It is important to select these correctly as they impact DI performance during the scanning and indexing process. Selecting the wrong worker nodes can slow scanning times and overwork the indexers.

Configuration also requires authorizing DI to access the Box account to scan files located on Box using the administrative username and password of an Enterprise Box account. These credentials are verified and authorized directly from DI on the authorization screen using **Authorize** button on the setting screen (Figure 1).



Log in to grant access to Box

Figure 1 – Box Authorization Screen

Authentication

DI monitors files by authenticating to the customer's Enterprise Box application using the OAuth2 protocol. Leveraging the OAuth2 protocol for authentication, DI saves a single OAuth2 token in the DI database. This token allows administrators to share their login credentials between DI and Box, which creates a connection between the two. When authentication from DI to Box is confirmed and a connection is established, DI services check the files on Box and record metadata information for each of the files.

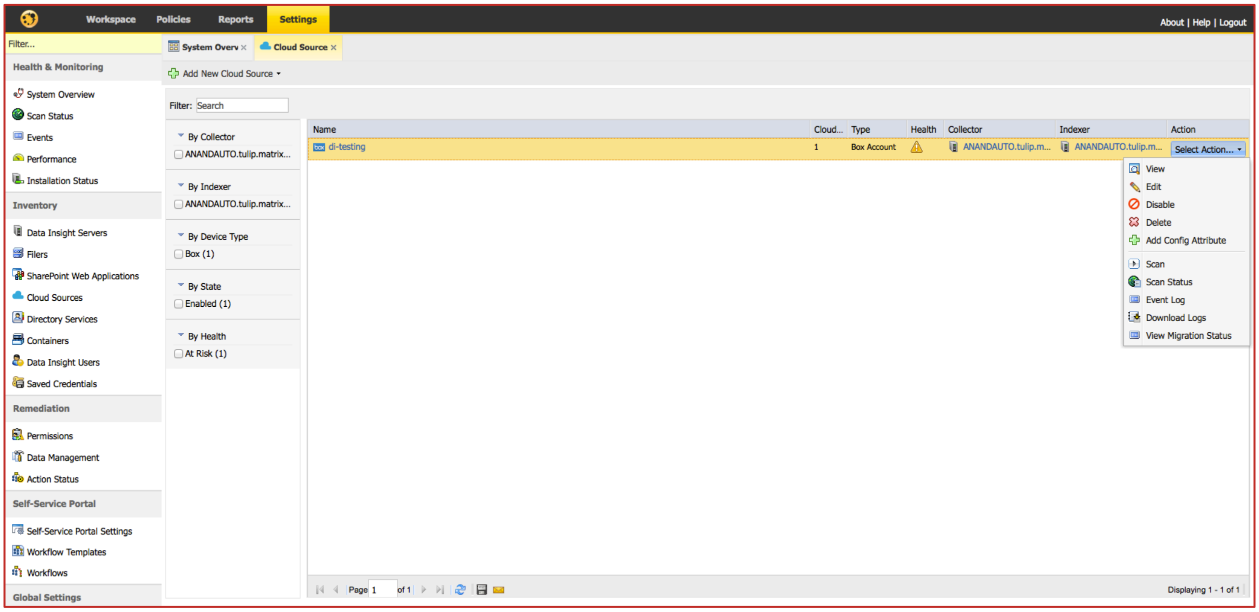
Scanning

Scanning occurs on a scheduled basis. During the Box to DI configuration, the DI administrator defines a scanning schedule for shares of the Box account. The DI administrator chooses one of the following:

- Use **Collector**’s default scanning schedule
- Use custom schedule

DI periodically scans the Box account to obtain file metadata. Each Collector worker node, by default, initiates a full scan of shares on the last Friday of each month at 7:00 P.M. (19:00). With Box accounts, incremental scans are not available.

Administrators can override the schedule anytime using the **Scan** action from the Cloud Sources list of the configured Box account (Figure 2).



Name	Cloud...	Type	Health	Collector	Indexer	Action
di-testing	1	Box Account	⚠	ANANDAUTO.tulip.m...	ANANDAUTO.tulip.m...	Select Action...

Figure 2 – Scanning a Box account

Indexing

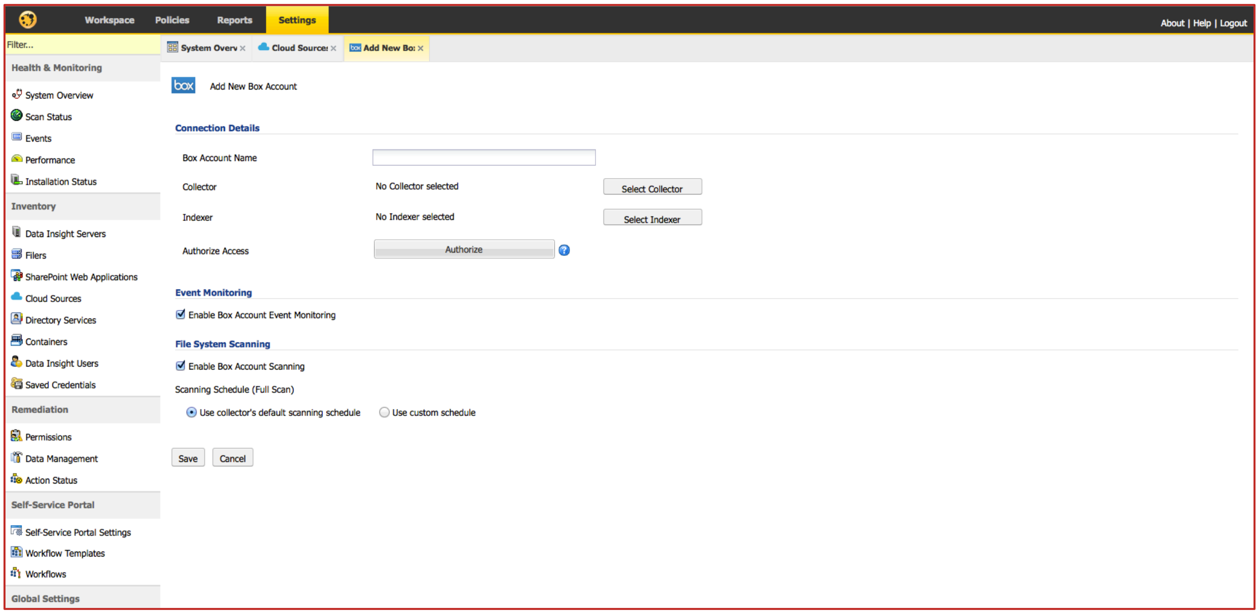
Unlike other shares, file metadata related to Box shares record actions differently. Since files are downloaded for editing, and then uploaded again when complete, DI translates these actions into usable metadata as outlined in the following table:

Term	DI definition
Read	Files downloaded from Box
Write	Files uploaded to the Box share
Share owner	User who created the shared folder in Box
File owner	User who uploaded the original file

Guided Tour

Add Box Account to Data Insight

Before Box folder and file scanning can take place, an Enterprise Box account must be synchronized with DI. An Enterprise account is required as it is the only Box account that can obtain information via the API that connects DI and Box. This can be configured in the DI interface **Settings > Cloud Services** section (Figure 3). The administrator can either use the existing **Collector** and **Indexer** configured during the installation or select one from the **Connection Details** options.



Add New Box Account

Connection Details

Box Account Name

Collector: No Collector selected

Indexer: No Indexer selected

Authorize Access

Event Monitoring

☑ Enable Box Account Event Monitoring

File System Scanning

☑ Enable Box Account Scanning

Scanning Schedule (Full Scan)

● Use collector's default scanning schedule ○ Use custom schedule

Figure 3 – Adding Box Account to Data Insight

To authorize access between DI and Box, the Box administrator credentials are used to secure a login. DI uses these credentials to retrieve metadata on shares and files in Box.

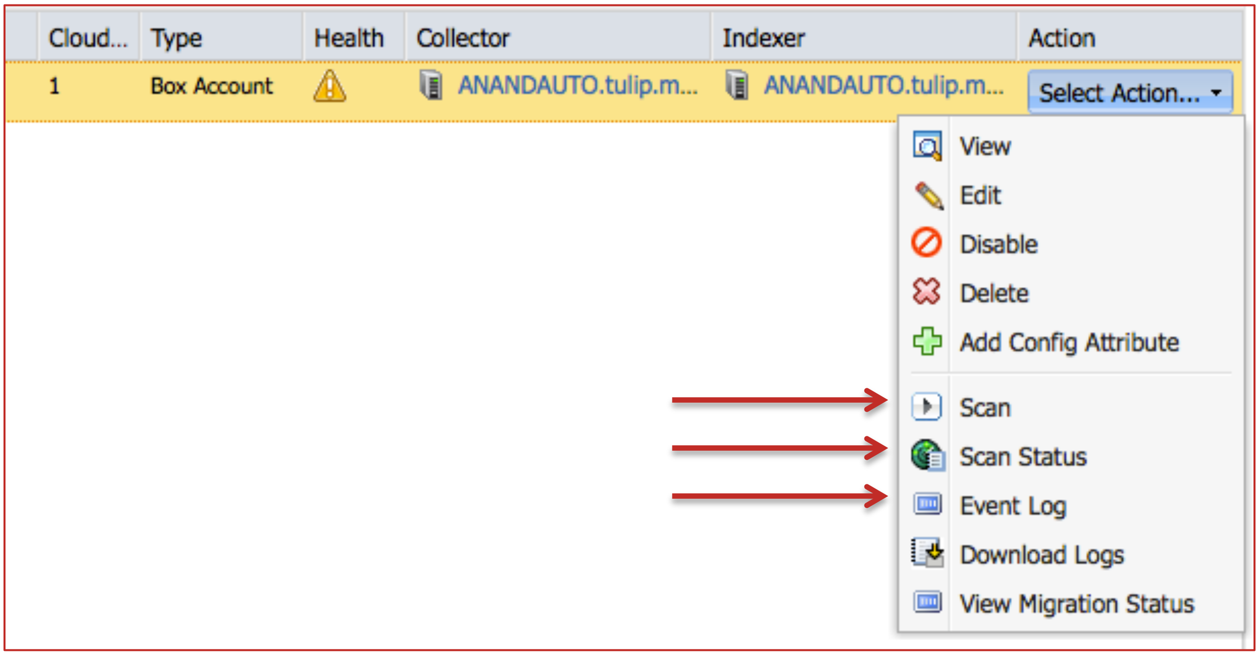
Audit Events

There are no additional configuration requirements for capturing audit events. Any user activities performed on Box shares appear in the raw audit files under the folder `<DI_DATA_DIR>/outbox`. The files are eventually consumed and indexed and the events display in the Data Insight console.

Scanning Box Accounts

By default, Box performs a full scan according to the scan schedule configured in DI – no incremental scans are available for Box. The scan schedule has an override on the **Settings** tab in the 'Cloud Sources' section (Figure 4). Administrators can also view:

- **Scan History**
- **Scan Errors**



Cloud...	Type	Health	Collector	Indexer	Action
1	Box Account	⚠	ANANDAUTO.tulip.m...	ANANDAUTO.tulip.m...	Select Action...

Figure 4 – Scanning Box Accounts

Licensing and support considerations

To scan Box shares, customers must purchase an additional license for Box scanning with Symantec Data Insight. Customers will only be able to scan Box folders and files with the purchase of this license.

Users' Box accounts should be provisioned against the users email addresses in Active Directory. This ensures Symantec Data Insight matches the correct identity in Box.

Symantec Data Insight scan of Box shares has the following limitations:

- Additional licensing is required for Symantec Data Insight to scan Box shares.
- Only one Enterprise Box account can be configured to Data Insight at a time.
- Portal activities are available for Box shares, except for incident remediation activities.
- The following options are not available on Box shares:
    - Permissions reporting
    - Entitlement review

About Symantec:
Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site: **www.symantec.com**

Symantec Corporation

World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA

+1 (650) 527 8000
+1 (800) 721 3934

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.