Forcepoint Dynamic Data Protection Getting Started Guide

Getting Started Guide | Forcepoint Dynamic Data Protection | 23-Aug-2019

Dynamic Data Protection is a Forcepoint Risk-Adaptive Protection solution that comprises the following Forcepoint security products or components:

- Forcepoint DLP
- Forcepoint One Endpoint (Forcepoint DLP endpoint)
- Forcepoint Behavioral Analytics (formerly Forcepoint UEBA)

See your product release notes for the specific product versions supported with Dynamic Data Protection.

Dynamic Data Protection combines the data security collection capabilities in Forcepoint DLP and its associated Forcepoint One Endpoint with the human-centric analytics in Forcepoint Behavioral Analytics to provide an administrator with risk-level profiles for specified individuals or groups. The administrator can then create different DLP action plans to trigger for each risk level.

This Getting Started Guide assumes that Forcepoint DLP version 8.5.2, 8.6.0, or 8.7.0 is already installed, properly configured, and running. Ensure that all DLP servers are also upgraded to version 8.5.2, 8.6.0, or 8.7.0. Contact Forcepoint Professional Services regarding a Forcepoint DLP version 8.5.2 patch that resolves an inconsistent risk level update issue.

Dynamic Data Protection workflow

The following general workflow describes Dynamic Data Protection functionality:

- A Forcepoint DLP administrator enables Forcepoint Risk-Adaptive Protection in the Data Security module and then configures Forcepoint Risk-Adaptive Protection policy rules to apply to users.
- The DLP administrator specifies DLP users or groups as Forcepoint Risk-Adaptive Protection users or groups using the Forcepoint Risk-Adaptive Protection User Manager.
- The Data Security module sends all DLP users to the Forcepoint Behavioral Analytics system, whether they are monitored by Forcepoint Risk-Adaptive Protection or not. This operation is performed on a predefined schedule or via a manual LDAP user directory import in the Forcepoint DLP Data Security module. The update may take some time, depending on the directory size.
- Forcepoint Behavioral Analytics receives Forcepoint DLP incident data and Forcepoint One Endpoint event data for all defined users.

- Forcepoint Behavioral Analytics analyzes user data and calculates a risk level for each monitored user (from 1 - 5, where 5 indicates most risk), which it then sends to Forcepoint DLP.
- Forcepoint DLP uses the risk level designation to determine action plan behavior in its policies for the specified users.

General configuration involves the following activities across the Dynamic Data Protection deployment. Steps **must** be performed in this order:

1. *Install and configure Forcepoint One Endpoint*
2. *Generate a valid certificate in Forcepoint DLP*
3. *Install Forcepoint UEBA and import valid certificate*
4. *Specify users or groups in the Forcepoint Risk-Adaptive Protection User Manager*
5. *Enable Forcepoint Risk-Adaptive Protection in Forcepoint DLP*
6. *Configure Forcepoint Risk-Adaptive Protection rules in Forcepoint DLP*
7. *Configure Forcepoint Behavioral Analytics integration with Forcepoint DLP*

Install and configure Forcepoint One Endpoint

Forcepoint DLP must already be installed and running before you install the Forcepoint One Endpoint. Ensure that any existing Forcepoint endpoints are removed from your system before you install Forcepoint One Endpoints. Only the Forcepoint One Endpoint is supported for Dynamic Data Protection.

See the following Endpoint product documentation for installation and configuration information:

- Forcepoint One Endpoint Release Notes
- Installing Forcepoint One Endpoint
- Forcepoint One Endpoint End User Guide

Generate a valid certificate in Forcepoint DLP

This step must be performed before you attempt to connect Forcepoint DLP to Forcepoint Behavioral Analytics. A Forcepoint DLP script generates an intermediate CA, which is then imported into Forcepoint Behavioral Analytics.

Warning

The process described in this section must be performed by a member of the Forcepoint Professional Services group. Please contact your Forcepoint representative for details.

Use the following steps to generate the required certificate files in Forcepoint DLP:

1. Log on to the Forcepoint DLP management server as Administrator.
2. Download the following two files to a temporary directory (e.g., C:\tools):
   - **runner.exe**
   - **UEBACertificateCreator.bat**
3. Open a Windows command prompt and change directory (cd) to the downloads directory (e.g., C:\tools).
4. Execute the following command from C:\tools:

   ```
   runner.exe UEBACertificateCreator.bat
   ```

   You can disregard any warnings about a missing **openssl.cnf** file during script execution.
5. This operation generates the following files in C:\temp\certs\ueba:
   - **ca.cer**
   - **ca.key**
   - **ueba.cer**
   - **ueba.key**

Important

After the Forcepoint Behavioral Analytics certificate import process is complete, we recommend that you delete the contents of the following directory for security reasons:

C:\temp\certs\ueba

Install Forcepoint UEBA and import valid certificate

You must install Forcepoint UEBA with the certificate files generated in Forcepoint DLP (see the previous section). See Forcepoint Behavioral Analytics Installation Manual for product installation information.

Warning

The process described in this section must be performed by a member of the Forcepoint Professional Services group. Please contact your Forcepoint representative for details.

Use the following steps to import the certificates generated in Forcepoint DLP to Forcepoint Behavioral Analytics:

1. Log on to your Forcepoint Behavioral Analytics Jenkins server using ssh.
2. Copy the certificate files you generated (ca.cer, ca.key, ueba.cer, ueba.key) into the following directory:

/etc/ansible/dlp-certs/

3. Update the /etc/ansible/group_vars/all directory with the following values:

```
##Place in DLP the external IP address of the Kafka service
kafka_external_ip: <external IP of kafka>
## Use DLP Provided Cert Chain
## We store files locally on jenkins
external_ca_certs: true
#external_ca_scheme: https
external_root_ca_cert_url:
"file:///etc/ansible/dlp-certs/ca.cer"
external_int_ca_key_url:
"file:///etc/ansible/dlp-certs/ueba.key"
external_int_ca_cert_url:
"file:///etc/ansible/dlp-certs/ueba.cer"
```

4. Remove the Forcepoint Behavioral Analytics certificate chain and all host and service certificates/keys using the following command:

```
ansible-playbook /usr/share/ro-ansible/remove-crts.yml
```

5. Generate a Forcepoint Behavioral Analytics certificate chain. See the topic titled *Deployment - Manually Run Ansible Playbooks* in the Forcepoint Behavioral Analytics Installation Manual.

Specify users or groups in the Forcepoint Risk-Adaptive Protection User Manager

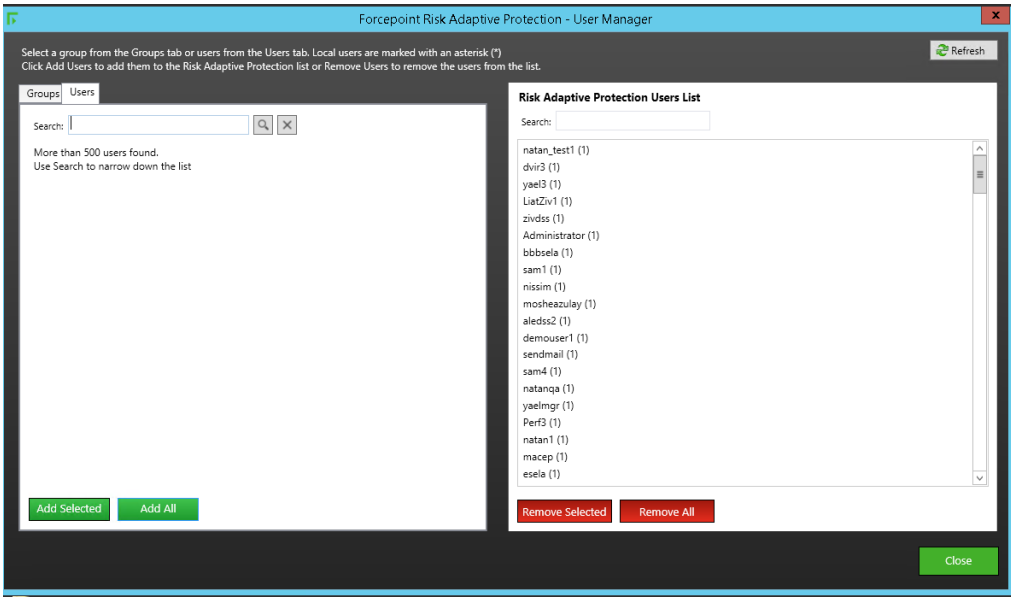
Forcepoint DLP users and groups are not designated Forcepoint Risk-Adaptive Protection users by default. The Data Security administrator must manually add users or groups in the Forcepoint Risk-Adaptive Protection User Manager. Then, the Data Security administrator imports the users into Forcepoint Behavioral Analytics.

See the Forcepoint Risk Adaptive Protection Tool User Guide for the tool's download and configuration information. Basic instructions for adding users or groups are included here for quick reference.

Use the following steps to select users or groups for Forcepoint Risk-Adaptive Protection analysis:

1. Log in to the Forcepoint Risk-Adaptive Protection User Manager.

2. Click **Refresh** to populate the Groups and Users tabs on the left with currently defined DLP groups and users.



Note

If the number of users in the Users tab exceeds a user-configured threshold, the complete list of users is not displayed, and the following message appears in the Users tab:

More than <*x*> users found. Use Search to narrow down the list.

Enter user name text in the Search field to display matching user name list entries.

This behavior affects only the Users tab. It does not apply to the Groups tab.

See the Forcepoint Risk Adaptive Protection Tool User Guide for more details.

3. Use one of the following methods to add users to the Forcepoint Risk-Adaptive Protection Users List:
   - Select the desired user names in the Users tab and click **Add Selected**.
   - Enter user names in the Search field, select the desired user names, and click **Add Selected**.
   - Click **Add All** to transfer all users to the Forcepoint Risk-Adaptive Protection Users List.

4. To add groups to the Forcepoint Risk-Adaptive Protection Users List, select the desired group names in the Groups tab and click **Add Group's Users**.

   A Search facility allows you to search for specific names.

> **Important**
>
> Users are not automatically imported into Forcepoint Behavioral Analytics after these steps. Users may be imported via:
>
> - A scheduled nightly LDAP user update in Forcepoint DLP (see *Scheduled LDAP imports*, page 7, for details)
> - A manual LDAP update from the Data Security module (see *Manual LDAP import*, page 8, for details)
>
>   For the initial update, we recommend that you run a manual update.
>
>   This process may take a long time, depending on the size of the LDAP directory database.
>
> In the event that the connection between Forcepoint DLP and Forcepoint Behavioral Analytics is interrupted, the LDAP import process may fail or send only a partial update without notifying the administrator. A subsequent import attempt (scheduled or manual) may be successful.

Use these steps each time you add Forcepoint Risk-Adaptive Protection users. Be aware that the duration of the database update depends on the size of the directory.

You can remove users or groups from the Forcepoint Risk-Adaptive Protection Users List by selecting the desired user or group names and clicking **Remove Selected** or **Remove All**.

> **Note**
>
> You may observe that an **Add** or **Remove** button may start to blink continuously after you click it. The blinking behavior does not impact user manager **Add** or **Remove** functionality.

Enable Forcepoint Risk-Adaptive Protection in Forcepoint DLP

Use the following steps to enable Forcepoint Risk-Adaptive Protection in Forcepoint DLP:

1. Select the Forcepoint Risk-Adaptive Protection tab on the **Settings > General > Services** page.
2. Mark the **Enable Risk-Adaptive Protection** check box.
3. Enter the Forcepoint Behavioral Analytics hostname or IP address in the appropriate field.
4. Enter the port number (default is 9093).

   Ensure that your firewall is properly configured to allow the connection between Forcepoint DLP and Forcepoint Behavioral Analytics.
5. Click **Test Connection** to verify the connection between Forcepoint DLP and Forcepoint Behavioral Analytics.

   If the connection test is not successful, check the following items:

   - Network connectivity
   - Forcepoint Behavioral Analytics server settings (hostname, IP address, and port)
   - That the Forcepoint UEBA server is running
   - That a valid certificate is installed

   Note
   If you configured your Forcepoint Behavioral Analytics connection using a hostname (in step 3), you need to disable and then re-enable Forcepoint Risk-Adaptive Protection as described in step 2 after you successfully resolve your connection.

   Contact Forcepoint Technical Support if these measures do not resolve your issues.

   The Data Security module checks this connectivity periodically. Successful and unsuccessful connections are reported in the Data Security module System Log.
6. Click **OK** to save your entries.
7. Click **Deploy** to activate your settings.
8. Restart Windows Service: **Websense Data Security Batch Server**.

Forcepoint DLP actions are enforced only after the initial LDAP directory import is complete.

Changes to any Forcepoint Risk-Adaptive Protection configuration setting are recorded in the Data Security module Audit Log.

Scheduled LDAP imports

By default, LDAP import updates occur daily at 11:00 PM. You can change the default time for the import operation in the Forcepoint DLP Security Manager using the following steps:

1. In the **Settings > General > User Directories** page, click the Import daily link at the top right of the screen.
2. In the Schedule User Directory Import dialog box, select a daily or weekly import option and configure the new day or time, or both.

LDAP import updates may take some time, depending on the LDAP directory size.

Manual LDAP import

You can perform a manual LDAP import at any time in the Forcepoint DLP Security Manager. Because LDAP updates may take a long time, depending on the LDAP directory size, we recommend using this command during low traffic intervals.

Use the following steps:

1. In the **Settings > General > User Directories** page, mark the check box to the left of the user directory you want to update.
2. Click **Import Now** at the top of the screen to begin the import.

Configure Forcepoint Risk-Adaptive Protection rules in Forcepoint DLP

Create or modify DLP policies and rules to define action plans for Forcepoint Risk-Adaptive Protection users. Use the Policy Rule wizard in the Data Security module (**Main > Policy Management > DLP Policies**). (See Creating custom DLP policies in the Forcepoint DLP Administrator Help for detailed instructions on using the Policy Rule wizard.)

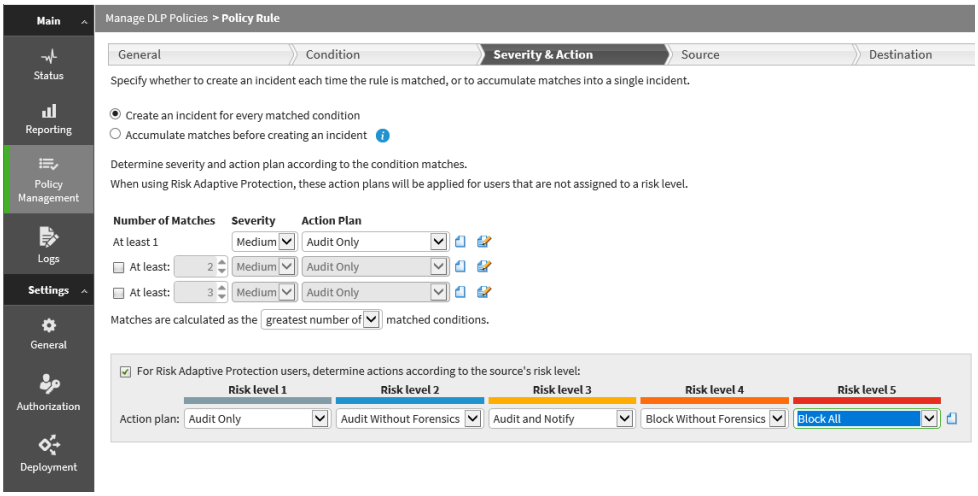
Use the Severity and Action tab in the Policy Rule wizard to configure Forcepoint Risk-Adaptive Protection policy actions based on a user's risk level determined by Forcepoint Behavioral Analytics analytics. Forcepoint DLP uses these settings when a rule is triggered.

Note

The Forcepoint UEBA risk level update to Forcepoint may take up to one hour, so an interval of inconsistent risk level between the two components is possible.

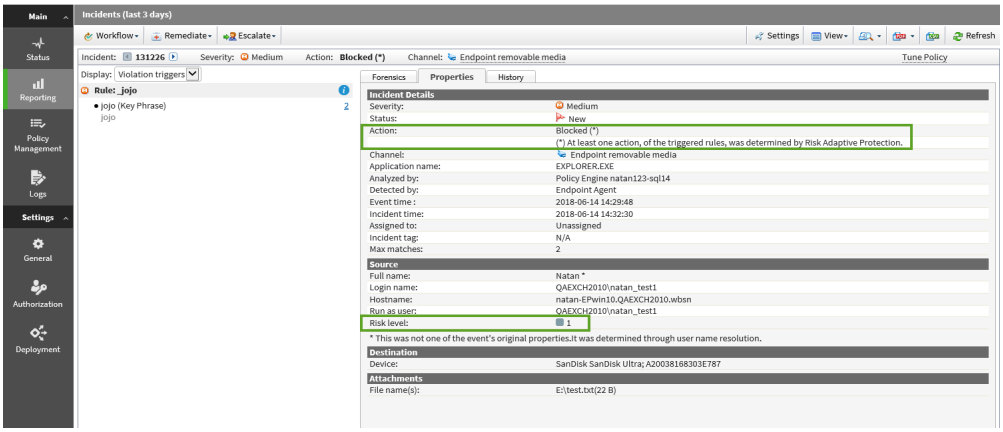
1. Mark the **For Risk-Adaptive Protection users, determine action according to the source's risk level** check box.

2. Select an action plan for each risk level from the Action plan drop-down lists at the bottom of the tab. This action applies only to specified Forcepoint Risk-Adaptive Protection users.

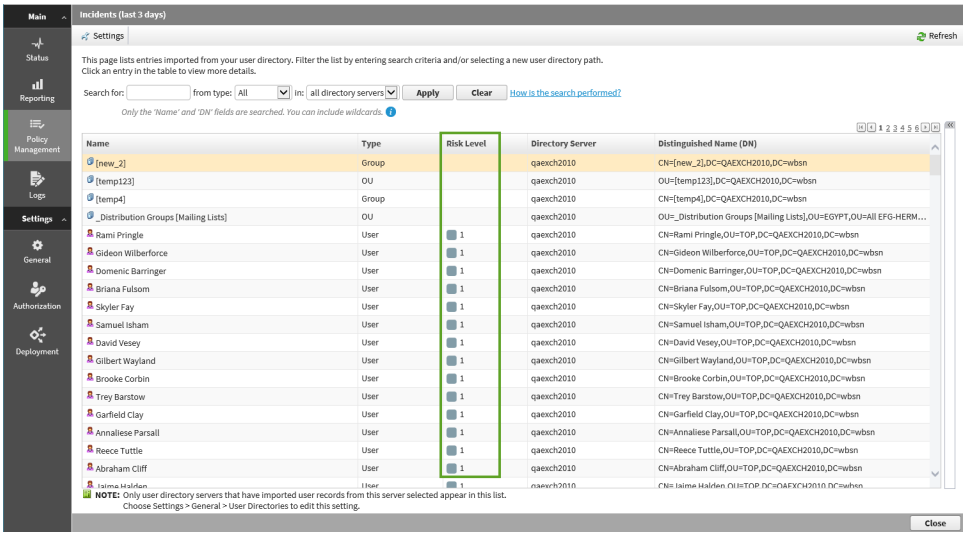


3. Complete the wizard and click **Finish**.

Incident properties include Forcepoint Risk-Adaptive Protection action and risk level in the Incidents list (**Main > Reporting > Data Loss Prevention > Incidents**). The following screen is in **View > Incident Preview Only** mode:



You can view a list of Data Security users along with each user's risk level in the User Directory Entries page (**Main > Policy Management > Resources > User Directory Entries**).



Configure Forcepoint Behavioral Analytics integration with Forcepoint DLP

Forcepoint DLP sends all its users to the Forcepoint Behavioral Analytics system, where entities are defined and tagged for monitoring. An entity may be a data item like a person, file, or network device. An entity attribute is data that describes the entity, like an office location or department membership.

Only monitored entities receive a risk score. You must specify the subset of DLP users on which you want to gather specific in-depth analytics

Note

A new entity that is designated for monitoring in Forcepoint Behavioral Analytics may not display a risk score until that entity generates some activities on which to calculate the score.

The Forcepoint Behavioral Analytics Attributes Card lists all of the applied Attributes of the specific Entity and allows administrators to create, edit, and remove Entity Attributes. The Attributes Card is also where Entities are designated as Monitored Entities, or as Entities that are scored. Attributes are useful for providing basic information about an Entity, such as their office location and job title.

There is no need to manually configure Dynamic Data Protection entities as "Monitored Entity = True". Forcepoint DLP automatically configures the value as True for entities for which it is collecting event information.

Note

If Monitored Entity values are set to False within Forcepoint Behavioral Analytics, continued integration with Forcepoint DLP may see those values set back to True as the Forcepoint DLP integration continues to share information for that entity with Forcepoint Behavioral Analytics.

Dynamic Data Protection in the Forcepoint Behavioral Analytics User Interface

Forcepoint Behavioral Analytics produces a risk score for all monitored entities, on a scale of 0-100, with 100 being the highest. When Dynamic Data Protection is active, Forcepoint Behavioral Analytics also produces a risk level for each monitored entity. The risk level is on a scale from 1 through 5, with 5 being the highest risk level.

Risk level is calculated based on a weighted average of the risk score over a window of time. The weighting favors more recent high scores over less recent low scores. Risk level is more likely to rise quickly and drop slowly. This increases risk level with recent high risk scores, and reverses that rise in risk level only as the risk score stays lower for a prolonged period of time.

Users with the Admin Role can manually adjust Risk levels for a selected timeframe from the Risk Level tab of the Entity page. This adjustment is made based on external information not available to the analytic platform, for instance, Human Resource information. After the selected duration of time, the risk level returns to the value calculated by the analytics configuration. Manual adjustments are logged and published in real time to Forcepoint DLP for Dynamic Data Protection update, but the adjustment is not reflected in the timelines until the next calculation period.

For detailed information about reviewing entity information in the Forcepoint Behavioral Analytics user interface, see the Forcepoint Behavioral Analytics User Manual.

Troubleshooting

Consider the following issues in the event that Forcepoint Risk-Adaptive Protection is not functioning properly:

- Verify Forcepoint DLP connectivity to Forcepoint Behavioral Analytics. In the **Settings > General > Services** Forcepoint Risk-Adaptive Protection tab, click **Test Connection**.

- View the Data Security module System Log for error or warning messages regarding system operation.
- Restart the following Windows services:
  - Websense Data Security Batch Server
  - Websense Data Security Message Broker
  - Websense Data Security Manager
- New keystore files may not be imported after any of the following activities:
  - Re-registering a secondary DLP server to a new management server machine
  - Backup/restore Forcepoint DLP to a new management server machine
  - Modify/repair Forcepoint DLP to a new management server machine

  Workaround:

  Use the following steps after the activity is completed:

  1. Delete the files in the following folder:

     ```
     C:\Program Files (x86)\Websense\Data
     Security\EPS_CAMEL\keystore
     ```

  2. Copy the file **cacerts.bcfks** from the original manager to the new DLP management server.
  3. Restart the following service:

     Websense DLP Endpoint Server to UEBA Connector
- You can view system health monitors to ensure that data is flowing properly between Forcepoint DLP and Forcepoint Behavioral Analytics.
  - The Forcepoint Behavioral Analytics application platform includes a monitoring server with dashboards that indicate system health for the various services included in Forcepoint Behavioral Analytics. View the monitoring dashboard to determine the overall health of the server that hosts the Forcepoint Behavioral Analytics service.
  - The Forcepoint DLP Data Security module monitors the data throughput for Forcepoint Behavioral Analytics. View system health on the **Main > Status > System Health** page for indications that traffic has halted for any reason.