



# User ID Service

2.5 or higher

**How to integrate Forcepoint User ID Service with other Forcepoint products**

© 2022 Forcepoint

Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.  
All other trademarks used in this document are the property of their respective owners.

Published 25 May 2022

Every effort has been made to ensure the accuracy of this document. However, Forcepoint makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Forcepoint shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

# Contents

<b>1 Introduction to the Forcepoint User ID Service</b> .....	7
Components.....	7
Example configuration of the User ID Service.....	10
High availability.....	10
Overview to integrating the User ID Service.....	11
<b>2 Installing the User ID Service</b> .....	13
Overview to installing the User ID Service.....	13
Requirements.....	14
Obtaining installation files.....	14
Prepare your environment.....	15
Install the User ID Service.....	17
<b>3 Perform initial setup of the User ID Service</b> .....	19
Start the initial setup.....	19
Configure the network details.....	20
Configure the basic TLS details.....	21
Add an API user during the initial setup.....	21
Add an LDAP server.....	22
<b>4 Configuring the User ID Service</b> .....	29
Using the Forcepoint User ID Service Configuration Utility.....	29
Start the Configuration Utility.....	30
Show the User ID Service configuration.....	32
Show the status of the User ID Service.....	33
Configure the UID Server.....	33
<b>5 Using the User ID Service API</b> .....	35
Overview to using the User ID Service API.....	35
Add additional API users.....	35
Delete an API user.....	36
Show all API users.....	36
<b>6 Configuring LDAP servers</b> .....	37
Add an Active Directory server.....	37
Add OpenLDAP server.....	39
Configure advanced TLS settings.....	40
Configure advanced Active Directory server settings.....	41
Configure advanced OpenLDAP server settings.....	42
Test the connection to LDAP servers.....	42
Configure global LDAP settings.....	43
Show the LDAP server configurations.....	44
Modify an LDAP server.....	44
Remove an LDAP server.....	45
Configure the LDAP server synchronization frequency.....	45
Synchronize with the LDAP server manually.....	47
Unlock an LDAP server.....	47
<b>7 Configuring certificates for the User ID Service</b> .....	49

Certificates used in the User ID Service.....	49
Configure LDIF hybrid cloud user synchronization.....	50
Using externally-signed certificates.....	52
Create a self-signed certificate.....	56
View the contents of the installed certificate.....	57
View the supported TLS versions and cipher suites.....	57
<b>8 Configuring the CockroachDB database.....</b>	<b>59</b>
Configure the CockroachDB database.....	59
Modify the expiration time of logon data.....	61
Query the database for a specific user, IP address, or security identifier.....	62
<b>9 Configuring logging for the User ID Service.....</b>	<b>63</b>
Select the log level.....	63
View User ID Service log events.....	65
Forwarding log data to the SMC.....	65
<b>10 Installing the DC Agent.....</b>	<b>71</b>
Overview to installing the DC Agent.....	71
Requirements.....	72
Obtaining installation files.....	72
Install the DC Agent.....	73
<b>11 Configuring the DC Agent.....</b>	<b>75</b>
Overview to configuring the DC Agent.....	75
Configure the User ID Service details.....	76
Configure which Domain Controllers and Exchange Servers to poll.....	76
Configure User ID Service credentials for the DC Agent.....	77
TLS certificates for the DC Agent.....	78
Modify the DC Agent service properties.....	79
Configuring advanced options.....	80
Troubleshooting the DC Agent.....	83
<b>12 Using the User ID Service and DC Agent in an HA configuration.....</b>	<b>85</b>
Introduction to using an HA configuration.....	85
Overview to configuring HA for the User ID Service.....	86
Overview to configuring HA for the DC Agent.....	91
<b>13 Integrating Forcepoint NGFW as the User ID Service Client Product.....</b>	<b>93</b>
Overview to configuring Forcepoint NGFW.....	93
Configuring certificates for Forcepoint NGFW.....	93
Create a Forcepoint User ID Service element.....	97
Select the Forcepoint User ID Service element for the NGFW Engine.....	99
Verifying that the SMC is receiving data from the User ID Service.....	100
<b>14 Maintenance.....</b>	<b>103</b>
Show the User ID Service version.....	103
Upgrade the User ID Service and the DC Agent.....	104
Uninstall the User ID Service and the DC Agent.....	107
Backing up and restoring the User ID Service configuration.....	109
Reset the User ID Service configuration.....	110
Collect configuration and server log data for troubleshooting.....	111
<b>A Appendix.....</b>	<b>115</b>

Default communication ports for the User ID Service..... 115  
Copyrights and trademarks..... 115



## Chapter 1

# Introduction to the Forcepoint User ID Service

### Contents

- [Components](#) on page 7
- [Example configuration of the User ID Service](#) on page 10
- [High availability](#) on page 10
- [Overview to integrating the User ID Service](#) on page 11

The Forcepoint User ID Service (User ID Service) collects data about groups, users, and associated IP addresses from Windows Active Directory (AD) Servers, OpenLDAP Servers, Microsoft Domain Controllers, Microsoft Exchange Servers, and external sources of user authentication.

The User ID Service API can also be used to provide data to the User ID Service.

When you integrate the User ID Service with another Forcepoint product, such as Forcepoint Next Generation Firewall (Forcepoint NGFW), you can use the user data from the User ID Service for access control and monitoring users.

## Components

---

Communication between the components is secured by TLS.

## User ID Service

---

The User ID Service receives domain, group, and user definitions, and associated IP address data from the DC Agent, Active Directory Servers or OpenLDAP and external authentication sources, and external authentication sources.

The UID Server and the CockroachDB database components are part of the User ID Service. The AD and OpenLDAP servers are represented as LDAP servers in the User ID Service configuration.

You can use the Forcepoint User ID Service Configuration Utility (Configuration Utility) to perform the initial setup and modify the User ID Service configuration.

### Related information

[Configuring the User ID Service](#) on page 29

## UID Server

The UID Server communicates with the DC Agent, AD and OpenLDAP Servers, the User ID Service Client Product with which the User ID Service has been integrated, and any other source of user or logon data that provides data using the User ID Service API.

### Related tasks

[Configure the UID Server](#) on page 33

## CockroachDB database

The CockroachDB database is an SQL database that stores data received through the User ID Service API from the DC Agent, AD and OpenLDAP server, and other sources of user or logon data.

In a high-availability (HA) configuration, the database is synchronized between cluster members. For more information about CockroachDB, go to <https://www.cockroachlabs.com>.

The CockroachDB database is populated through the User ID Service API. Other sources of user or logon data can use the User ID Service API to interact with the database. For more information, see the *Forcepoint User ID Service API User Guide*.

### Related information

[Configuring the CockroachDB database](#) on page 59

## LDAP server

The LDAP servers in the User ID Service configuration represent AD and OpenLDAP servers. The User ID Service acts as an LDAP client.

The User ID Service synchronizes domain, group, and user definitions from AD and OpenLDAP servers automatically on a set schedule. The schedule can be either at a specific time every day, or at regular intervals. You can also manually synchronize the data.

### Related information

[Configuring LDAP servers](#) on page 37

## Best practices for LDAP servers configuration

Follow these recommendations when you configure AD LDAP and OpenLDAP servers in the User ID Service configuration.

### AD LDAP Server configuration

Perform the following step to configure AD LDAP servers:

- Add an LDAP server for each domain in the AD forest.  
To synchronize users and groups using the AD Global Catalog, use one of the following ports depending on your AD LDAP configuration:
  - 3286 (LDAP)



- 3269 (LDAPS)

To synchronize users and groups using the AD Local Catalog, use one of the following ports depending on your AD LDAP configuration:

- 389 (LDAP)
- 636 (LDAP)

If you synchronize users and groups with the AD Global Catalog, the LDAP server for the root domain of any AD tree will retrieve all users and all groups from the whole AD tree, except Domain Local Groups. To retrieve all Domain Local Groups, you must add a FUID LDAP server configuration for each server in your AD tree.

### **OpenLDAP Server configuration**

Perform the following step to configure the OpenLDAP servers:

- Add LDAP servers for each domain in your OpenLDAP definition.  
To synchronize users and group use one of the following ports depending on your OpenLDAP server configuration:
  - 389
  - 636

## **DC Agent**

---

The DC Agent is a Microsoft Windows application that collects user authentication events from Microsoft Domain Controllers (DC) and Microsoft Exchange Servers.

The DC Agent provides data about users and associated IP addresses to the User ID Service.

You can install one or more instances of the DC Agent in the same AD domain.

### **Related information**

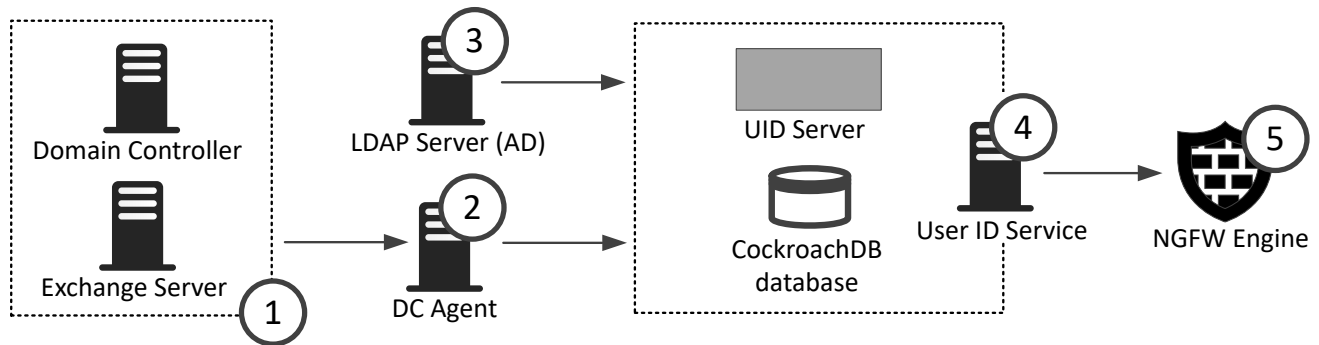
[Configuring the DC Agent on page 75](#)

## User ID Service Client Product

The User ID Service Client Product is the Forcepoint product with which the User ID Service has been integrated. It receives domain, group, and user definitions, and associated IP addresses from the User ID Service.

# Example configuration of the User ID Service

In this example, the Forcepoint NGFW is the User ID Service Client Product.



- 1 The Domain Controller and Exchange Server provide data about user logon events and associated IP addresses to the DC Agent.
- 2 The DC Agent uses the User ID Service API to provide collected data from the Domain Controller and Exchange Server to the User ID Service.
- 3 The AD Server provides data about domain, group, and user definitions to the UID Server, which populates the CockroachDB database with this data. The AD Server is represented in the User ID Service as an LDAP server, and the UID Server acts as an LDAP client.
- 4 The UID Server and the CockroachDB database components are part of the User ID Service. The UID Server communicates with other components. The database contains domain, group, and user definitions, and associated IP addresses.
- 5 The Forcepoint NGFW polls data about groups, users, and associated IP addresses from the UID Server.

### Related information

[Integrating Forcepoint NGFW as the User ID Service Client Product](#) on page 93

## High availability

You can use the User ID Service in a high-availability (HA) configuration.

In an HA configuration, you install the User ID Service on additional servers, and the CockroachDB is synchronized between the cluster members. You can also install more than one instance of the DC Agent.

### Related information

[Using the User ID Service and DC Agent in an HA configuration on page 85](#)

# Overview to integrating the User ID Service

Complete the following high-level steps to integrate the User ID Service with other Forcepoint products.

- 1) Obtain the installation files for the User ID Service and DC Agent.
- 2) Prepare your environment for installing the User ID Service.
- 3) Install the User ID Service.
- 4) Perform the initial setup of the User ID Service.
- 5) To use the User ID Service in an HA configuration, install and perform the initial setup of the User ID Service on additional servers.
- 6) Add an API user for the DC Agent to use for interacting with the User ID Service.
- 7) Configure the certificates needed for secure communication between the User ID Service components and between the User ID Service and the User ID Service Client Product.
- 8) Install and configure the DC Agent.
- 9) To use the DC Agent in an HA configuration, install the DC Agent on an additional server.
- 10) In the User ID Service Client Product, such as Forcepoint NGFW, configure the User ID Service settings.

### Related information

[Installing the User ID Service on page 13](#)

[Perform initial setup of the User ID Service on page 19](#)

[Using the User ID Service and DC Agent in an HA configuration on page 85](#)

[Using the User ID Service API on page 35](#)

[Configuring certificates for the User ID Service on page 49](#)

[Installing the DC Agent on page 71](#)

[Configuring the DC Agent on page 75](#)

[Integrating Forcepoint NGFW as the User ID Service Client Product on page 93](#)



## Chapter 2

# Installing the User ID Service

### Contents

- Overview to installing the User ID Service on page 13
- Requirements on page 14
- Obtaining installation files on page 14
- Prepare your environment on page 15
- Install the User ID Service on page 17

Install the User ID Service on a CentOS or Red Hat Enterprise Linux server.

## Overview to installing the User ID Service

---

Complete the following high-level steps to install the User ID Service.

- 1) Obtain the installation file.
- 2) Prepare your environment.
- 3) Install the User ID Service.

To use the User ID Service in an HA configuration, you must install and configure the User ID Service on additional servers. For more information, see the separate section about HA configuration.

# Requirements

---

See the [Release Notes](#) for information about hardware and system requirements for the User ID Service and the DC Agent for the Forcepoint User ID Service.

## Obtaining installation files

---

Download the installation files, then check the file integrity.

### Download installation files

---

Download the installation files from the Forcepoint website.

- The User ID Service installer is provided as a .run file.
- The DC Agent installer is provided as a .exe file.

#### Steps

- 1) Go to <https://support.forcepoint.com/Downloads>.
- 2) Enter your license code or log on using an existing user account.
- 3) Click **All Downloads**, then browse to the **Network Security** section.
- 4) Under **User ID Service**, select **All versions**.
- 5) Download the installers for the version that you want to install.



#### Important

Download the same version of the User ID Service and DC Agent installers.

### Check the file integrity

---

Before running the installers, check that the installer files have not become corrupt or been changed. Using corrupt files might cause problems at any stage of the installation and use of the system.

#### Steps

- 1) Look up the correct checksum in the [Release Notes](#) or on the Downloads page at <https://support.forcepoint.com/Downloads>.
- 2) Open a command prompt, then go to the directory where you saved the installer file.

- 3) Generate a checksum of the file, where `<filename>` is the name of the installation file.  
From a Linux command prompt, enter:

```
sha256sum <filename>
```

From a Windows PowerShell prompt, enter:

```
Get-FileHash <filename>
```

- 4) Verify that the checksum matches the checksum listed in the Release Notes or on the Downloads page.



#### CAUTION

Do not use files that have invalid checksums. If downloading the files again does not help, contact [Forcepoint Customer Hub](#).

## Prepare your environment

You must prepare your environment before you install the User ID Service.

### Before you begin

Carefully read the hardware requirements and system requirements for the User ID Service in the [Release Notes](#).

Configure the CentOS or Red Hat Enterprise Linux host firewall to allow incoming connections from the DC Agent and from clients, such as NGFW Engines and User ID Service API users, to the User ID Service server.

#### Related concepts

[Default communication ports for the User ID Service on page 115](#)

## Configure the host firewall

The host firewall blocks incoming connections from the DC Agent and the clients unless you allow the connections. You must also make sure that all firewalls between the components, including the host firewalls, allow the communications.

In this example configuration, the following components are used:

- Install DC Agent version 2.0 or higher.
- Three components that act as clients of the User ID Service:
  - An installation of DC Agent version 2.0 or higher.
  - A Forcepoint NGFW Engine.
  - An additional client that uses the User ID Service API to connect to the User ID Service.
- Three User ID Service cluster members in an HA configuration.

Replace the IP addresses used in this example with the IP addresses used in your environment.

## Steps

- 1) To view the current firewall configuration, enter the following command:

```
sudo firewall-cmd --get-active-zones
```

- 2) To view the details of a specific zone, enter the following command:

```
firewall-cmd --info-zone=<zone name>
```

Where `<zone name>` is the name of the zone.

- 3) Create a zone that allows communication with components that act as clients of the User ID Service. The components are DC Agent version 2.0 or higher, a Forcepoint NGFW Engine, and an additional User ID Service API client.

Enter the following commands:

```
sudo firewall-cmd --permanent --new-zone=uidclient
sudo firewall-cmd --permanent --zone=uidclient --add-source=10.11.12.1/32
sudo firewall-cmd --permanent --zone=uidclient --add-source=10.11.13.1/32
sudo firewall-cmd --permanent --zone=uidclient --add-source=10.11.14.1/32
sudo firewall-cmd --permanent --zone=uidclient --add-port=5000/tcp
```

- 4) Create a zone that allows the nodes in an HA configuration to communicate with each other.

Enter the following commands:

```
sudo firewall-cmd --permanent --new-zone=uid
sudo firewall-cmd --permanent --zone=uid --add-source=10.0.0.101/32
sudo firewall-cmd --permanent --zone=uid --add-source=10.0.0.102/32
sudo firewall-cmd --permanent --zone=uid --add-source=10.0.0.103/32
sudo firewall-cmd --permanent --zone=uid --add-port=26257/tcp
```

- 5) If you want to access the CockroachDB database dashboard, create a zone for that.

Enter the following commands:

```
sudo firewall-cmd --permanent --new-zone=cockroachweb
sudo firewall-cmd --permanent --zone=cockroachweb --add-source=10.0.100.51/32
sudo firewall-cmd --permanent --zone=cockroachweb --add-port=8080/tcp
```

- 6) Enable the new configuration.

Enter the following command:

```
sudo firewall-cmd --reload
```

- 7) If the firewall is disabled, re-enable the firewall.

Enter the following command:

```
sudo systemctl start firewalld.service
```



# Install the User ID Service

Use the installation file to install the User ID Service.

## Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.
- 2) In the directory where you saved the User ID Service `.run` installation file, enter the following command:

```
bash <installer-name>
```

- 3) Press **Enter** to scroll through the License Agreement, then enter `Y` to accept the agreement.
- 4) Select **Install**.
- 5) When prompted to confirm your action, enter `Y`.

## Result

The User ID Service is installed.

## Next steps

Perform the initial setup using the `fuid-cfg setup` command in the Forcepoint User ID Service Configuration Utility.

### Related information

[Perform initial setup of the User ID Service on page 19](#)



## Chapter 3

# Perform initial setup of the User ID Service

### Contents

- Start the initial setup on page 19
- Configure the network details on page 20
- Configure the basic TLS details on page 21
- Add an API user during the initial setup on page 21
- Add an LDAP server on page 22
- Next steps after the initial setup on page 27

After installation of the User ID Service, use the Forcepoint User ID Service Configuration Utility (Configuration Utility) to perform the initial setup.

Complete the following high-level steps:

- 1) Set the role of the User ID Service as a standalone installation or as a cluster member in an HA configuration.
- 2) Configure the network details.
- 3) Configure the basic TLS details.
- 4) (Optional) Add an LDAP server that represents an AD or OpenLDAP Server.

## Start the initial setup

Use the Configuration Utility to perform the initial setup.



### Tip

Press **Ctrl+C** to cancel an action.

### Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.
- 2) Enter the following command:

```
fuid-cfg setup
```

3) Select the role of the User ID Service server.

Use the arrow keys to browse the list, then press **Enter** to make your selection.

Select from the following:

- **Initial cluster node** — Select this option if you are setting up an HA configuration, and this server is the first cluster member that you are configuring.
- **Join existing cluster** — Select this option if you are setting up an HA configuration, and another server was already configured as a cluster member.



**Important**

You must copy TLS certificates from another cluster member before you can join the cluster.

- **Standalone node** — Select this option if you are not setting up an HA configuration.

For more information about setting up an HA configuration, see the section about using the User ID Service in an HA configuration.

## Next steps

Configure the network details.

### Related information

[Using the User ID Service and DC Agent in an HA configuration on page 85](#)

# Configure the network details

Enter the network details to continue the configuration in the Configuration Utility.



**Tip**

In many cases, the default option is shown. To use the default option, press **Enter**.

## Steps

1) Enter the IP address of the UID Server.

The Configuration Utility detects the current IP address of the server and offers that IP address as the default.

The CockroachDB database also uses this IP address.

2) If the server is a cluster member in an HA configuration, enter a comma-separated list of IP addresses that represents the other cluster members.

The CockroachDB database uses the IP addresses to communicate with the cluster members. The number of IP addresses must be an odd number.

## Next steps

Configure the basic TLS settings.

# Configure the basic TLS details

---

Enter the basic TLS details to continue the configuration in the Configuration Utility.

A self-signed certificate is created to authenticate communication between the User ID Service and the User ID Service Client Product. In production environments, we do not recommend that you use the self-signed certificate to authenticate communications. Use the Configuration Utility to later add another certificate to the configuration.

## Steps

- 1) Enter the host name of the server to use as the common name in the certificate.  
The Configuration Utility detects the current host name of the server and offers that host name as the default. To use the default option, press **Enter**.
- 2) To specify a subjectAltName for the certificate, enter a comma-separated list of DNS names or IP addresses. This option is useful if multiple User ID Service Client Products need to communicate with the User ID Service, and specific peer identity values are required. To skip this step, press **Enter**.
- 3) To configure additional attributes for the certificate, enter **Yes**, then configure the attributes. To leave an attribute unspecified, press **Enter**.
  - a) Enter a two-letter country code.
  - b) Enter the name of the state or province.
  - c) Enter the name of the locality.
  - d) Enter the name of the organization.
  - e) Enter the name of the organizational unit.
- 4) To generate a certificate signing request (CSR) for the FUID server, select **Yes**.  
You can generate a self-signed unless a new server certificate replaces it. Forcepoint recommends generating the certificate signing request and have it signed by an external certificate authority.

## Next steps

Add an API user.

# Add an API user during the initial setup

---

To interact with or to populate the User ID Service database, create an API user for basic authentication.

After the initial setup of the User ID Service, you can use the Configuration Utility to add additional API users.

## Steps

- 1) Enter a user name for the API user.

- 2) Enter a password for the API user.
- 3) To add an LDAP server that represents an AD or OpenLDAP Server, enter **Y**. Otherwise, enter **N**.  
The AD or OpenLDAP Server is used to populate the User ID Service database with data about users and groups.

## Next steps

If you selected to add an LDAP server, continue the setup in the Configuration Utility.

Otherwise, you are shown a summary of the configuration. When prompted to confirm your action, enter **Y**.

If you do not add an LDAP server during the initial setup, you can use the Configuration Utility to later add one.

### Related tasks

[Add additional API users](#) on page 35

### Related information

[Configuring LDAP servers](#) on page 37

# Add an LDAP server

Add an LDAP server that represents an AD or OpenLDAP Server to continue the initial setup. You need to select the type of LDAP Server you want to configure.

For more information see [Add an Active Directory server](#) on page 22 and [Add an OpenLDAP server](#) on page 23.

## Add an Active Directory server

Add an LDAP server that represents an AD server to continue the initial setup.



### Tip

In many cases, the default option is shown. To use the default option, press **Enter**.

## Steps

- 1) Enter the IP address of the AD Server.
- 2) Enter the port that the AD Server listens on.  
The default port is 3268. For a secure LDAP (LDAPS) server, use port 3269.
- 3) Enter the base distinguished names (DN) for LDAP search.  
You can enter multiple base DNs on separate lines. Press **Enter** twice after you have entered the DNs.

- 4) Enter the user name of the account used to access the LDAP server.  
Enter the name in distinguished format. For example:

```
cn=administrator,cn=users,dc=example,dc=com
```

- 5) Enter the password of the account used to access the LDAP server.
- 6) To synchronize only users that have an email address, enter **Y**. Otherwise, enter **N**.  
You can use this option to, for example, avoid synchronizing service accounts that do not have email addresses associated with them.
- 7) To enable TLS encryption for the connection to the server, enter **Y**. Otherwise, enter **N**.
- 8) If you enabled TLS encryption, and want to enable strict TLS verification, enter **Y**. Otherwise, enter **N**.  
When enabled, you must have a CA installed that matches the CA on the AD Server. The CA and host name must match.
- 9) Configure NetBIOS Lookups. Select this option if the NetBIOS name of the AD server differs from the first DC component of the AD domain.  
It is not recommended to alter the default NetBIOS configuration, unless the AD server is using specialized configuration.
- 10) To configure advanced TLS or LDAP server settings, enter **Y**. Otherwise, enter **N**.

## Next steps

If you selected to configure advanced settings, continue the configuration in the Configuration Utility.

Otherwise, you are shown a summary of the configuration. When prompted to confirm your action, enter **Y**.

The User ID Service synchronizes with the LDAP server, populating the CockroachDB database.

### Related concepts

[Best practices for LDAP servers configuration](#) on page 8

## Add an OpenLDAP server

Add an LDAP server that represents an OpenLDAP server to continue the initial setup.

### Steps

- 1) Enter the IP address of OpenLDAP Server.
- 2) Enter the port that the OpenLDAP Server listens on.  
The default port is 389. For a secure LDAP (LDAPS) server, use port 636.
- 3) Enter the base distinguished names (DN) for LDAP search.  
You can enter multiple base DNs on separate lines. Press **Enter** twice after you have entered the DNs.

- 4) Enter the user name of the account used to access the LDAP server.  
Enter the name in the following sample format.

```
cn=administrator,cn=users,dc=example,dc=com
```

- 5) Enter the password of the account used to access the LDAP server.
- 6) To synchronize only users that have an email address, enter **Y**, else enter **N**.  
You can use this option to avoid synchronizing service accounts that do not have email addresses associated with them.
- 7) To enable TLS encryption for connecting to the server, enter **Y**, else enter **N**.
- 8) To enable strict TLS verification after enabling TLS encryption, enter **Y**, else enter **N**.  
When enabled, you must have a CA installed that matches the CA on the OpenLDAP Server. The CA and host name must match.
- 9) To configure advanced TLS or LDAP server settings, enter **Y**, else, enter **N**.

## Configure advanced Active Directory server settings

If you selected to configure advanced settings, continue the configuration in the Configuration Utility.



### Tip

In many cases, the default option is shown. To use the default option, press **Enter**.

We recommend you change the defaults only if you are familiar with the advanced configuration of LDAP servers.

### Steps

- 1) Enter the SID attribute of the LDAP server.  
The default value is `objectSid`.
- 2) Enter the GUID attribute of the LDAP server.  
The default value is `objectGUID`.
- 3) Enter the SAM account name of the LDAP server.  
The default value is `sAMAccountName`.
- 4) Enter the MemberOf attribute of the LDAP server.  
The default value is `memberOf`.
- 5) Enter the NTLM user name of the LDAP server.  
The default value is `NTLMIdentity`.



- 6) Enter the Mail attribute of the LDAP server.  
The default value is `mail`.
- 7) Enter the User Filter attribute of the LDAP server.  
The default value is `(&(objectCategory=person)(objectclass=user))`.
- 8) Enter the Group Filter attribute of the LDAP server.  
The default value is `(&(objectCategory=group)(objectclass=group))`.
- 9) Enter the size of the LDAP search page for the LDAP server.  
The default value is `1000`.

## Next steps

When you are shown a summary of the configuration, enter `y` to confirm your action.

The User ID Service synchronizes with the LDAP server, populating the CockroachDB database.

# Configure advanced OpenLDAP server settings

If you selected to configure advanced settings, continue the configuration in the Configuration Utility.



### Tip

In many cases, the default option is shown. To use the default option, press **Enter**.

We recommend you change the defaults only if you are familiar with the advanced configuration of LDAP servers.

## Steps

- 1) Enter the Primary User Attribute. This value represents a unique user attribute in the LDAP definition.  
The default value is `cn`.
- 2) Enter the Primary Group Attribute. This value represents a unique group attribute in the LDAP definition.  
The default value is `cn`.
- 3) Enter the Mail attribute of the LDAP server.  
The default value is `mail`.
- 4) Enter the User Filter attribute of the LDAP server.  
The default value is:  
`((|(objectclass=inetOrgPerson)(objectclass=person) (objectclass=organizationalPerson)))`
- 5) Enter the Group Filter attribute of the LDAP server.  
The default value is:  
`((|(objectclass=groupOfNames)(objectclass=country) (objectclass=organization) (objectclass=organizationalUnit)))`

- 6) Enter the size of the LDAP search page for the LDAP server.  
The default value is 1000.

## Configure advanced TLS settings

If you selected to configure advanced settings, continue the configuration in the Configuration Utility.



### Tip

In many cases, the default option is shown. To use the default option, press **Enter**.

### Steps

- 1) Enter the path to the location of the trusted CA file.  
The default location is the system CA store.
- 2) Select the cipher suites to use.  
Use the arrow keys to browse the list, press **Space** to make your selections, then press **Enter** to finish making your selection. To use the default list of ciphers, press **Enter**.  
The User ID Service uses the Go Language TLS module. TLS 1.3 algorithms are used first, then TLS 1.2 algorithms. For more information, see <https://golang.org/pkg/crypto/tls/>.
- 3) Select the minimum TLS version to use.  
Use the arrow keys to browse the list, then press **Enter** to make your selection.
- 4) To enable revocation checking, enter **Y**. Otherwise, enter **N**.  
When you enable revocation checking, all server certificates are checked against denied certificate revocation lists (CRL) and online certificate status protocol (OCSP). Revocation information must be included in the certificate. You cannot use CRLs for checking LDAP URLs. Only HTTP URLs are supported.
- 5) If you enabled revocation checking, select the default action if a certificate has been revoked.  
Use the arrow keys to browse the list, then press **Enter** to make your selection.
- 6) To enable peer identity checking, enter **Y**. Otherwise, enter **N**.
- 7) If you enabled peer identity checking, select the peer certificate attribute to match against.  
Use the arrow keys to browse the list, then press **Enter** to make your selection.
- 8) If you enabled peer identity checking, enter the value for the peer certificate attribute to match against.

### Next steps

Configure the advanced LDAP server settings in the Configuration Utility.

# Next steps after the initial setup

---

After performing the initial setup, we recommend that you do the following.

- Add an API user for the DC Agent to use for interacting with the User ID Service.

## **Related tasks**

[Add additional API users on page 35](#)



## Chapter 4

# Configuring the User ID Service

### Contents

- Using the Forcepoint User ID Service Configuration Utility on page 29
- Start the Configuration Utility on page 30
- Show the User ID Service configuration on page 32
- Show the status of the User ID Service on page 33
- Configure the UID Server on page 33

After performing the initial setup of the User ID Service, you can use the Configuration Utility to configure most of the settings.

## Using the Forcepoint User ID Service Configuration Utility

There are various commands for tasks that you can complete in the Configuration Utility.

Command	Description
api	Manage User ID Service API users. You must create an API user for the DC Agent to use. You can use the API to add, modify, or remove data from the CockroachDB database. For more information, see the <i>Forcepoint User ID Service API User Guide</i> in Knowledge Base article <a href="#">16151</a> .
backup	Back up the User ID Service configuration.
db	Configure the CockroachDB database.
help	Get help for specific commands.
ldap	Configure LDAP servers that represent the AD or OpenLDAP servers that send data about users and groups. You can also set how frequently the LDAP servers synchronize with the User ID Service.
ldif	Manage and configure LDIF user hybrid cloud syncing.
log	Set the log level for the User ID Service. You can also enable log forwarding between the User ID Service and the Forcepoint NGFW Security Management Center (SMC).
logon	Modify the expiration time of logon data. You can query the CockroachDB database for a specific user, IP address, or security identifier (SID).
metrics	Enable metrics for troubleshooting performance issues.
restore	Restore a backup of the User ID Service configuration.
setup	Perform the initial setup.
show	Show a summary of the current User ID Service configuration.

Command	Description
<code>status</code>	Show the current status of the User ID Service. You can also see the cluster members in an HA configuration.
<code>support</code>	Create a diagnostics file to provide to <a href="#">Forcepoint Customer Hub</a> .
<code>tls</code>	Manage certificates. You can create a self-signed certificate or certificate request, or import a signed certificate.
<code>uid</code>	Modify the configuration of the UID Server.

### Related tasks

- [Add additional API users on page 35](#)
- [Back up the configuration on page 109](#)
- [Configure the CockroachDB database on page 59](#)
- [Query the database for a specific user, IP address, or security identifier on page 62](#)
- [Get help for a command in the Configuration Utility on page 32](#)
- [Configure the IFMAP Server](#)
- [Add an Active Directory server on page 37](#)
- [Select the log level on page 63](#)
- [Enable forwarding log data to the SMC on page 65](#)
- [Modify the expiration time of logon data on page 61](#)
- [Enable metrics on page 112](#)
- [Restore the configuration on page 110](#)
- [Start the initial setup on page 19](#)
- [Show the User ID Service configuration on page 32](#)
- [Show the status of the User ID Service on page 33](#)
- [Collect configuration and server log data for troubleshooting on page 111](#)
- [Create a self-signed certificate on page 56](#)
- [Create a certificate request on page 54](#)
- [Import a signed certificate on page 55](#)
- [Configure the UID Server on page 33](#)

## Start the Configuration Utility

The Configuration Utility is a command-line tool that you can use to configure the User ID Service.

### Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.
- 2) Enter the following command:

```
fuid-cfg
```

## Result

A list of possible commands is shown.

# Global flags in the Configuration Utility

When entering a command in the Configuration Utility, you can add flags for advanced options.

## Set the log level

When you enter a command, you can temporarily set the log level for that command.

### Steps

- 1) Add the following flag:

```
-L, --log-level [LEVEL]
```

Where [LEVEL] is one of the following:

- **FATAL** — Only fatal errors are logged.
- **ERROR** — Only errors are logged.
- **WARNING** — Only warnings are logged.
- **INFO** — Information that is generally useful is logged. This log level is the default log level.
- **DEBUG** — Information that is useful for support is logged.
- **TRACE** — All available information is logged.



#### Note

When you select a log level, both the logs of that level and higher are generated.

### Related tasks

[Show the log level on page 64](#)

## Disable restarting of services

When you enter a command, you are typically asked if you want to restart the associated services. If you do not want to restart services, you can add a flag.

### Steps

- 1) Add the following flag:

```
--no-restart
```



#### Note

Changes to the User ID Service configuration are not taken into use until services are restarted.

# Automatically accept all confirmation prompts

When you enter a command, you are sometimes asked to confirm your action. To automatically accept all confirmation prompts, you can add a flag.

## Steps

- 1) Add the following flag:

```
-y, --yes
```

# Get help for a command in the Configuration Utility

In addition to this document, you can also use the integrated help when using the Configuration Utility.

## Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.

- 2) Enter the following command:

```
fuid-cfg help [command]
```

When entering most commands, you can also use the following flag:

```
fuid-cfg [command] -h, --help
```

When entering information for an individual option, you can enter `?` to get help on the option.

# Show the User ID Service configuration

You can view a summary of the User ID Service configuration in the Configuration Utility.

## Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.

- 2) Enter the following command:

```
fuid-cfg show
```



## Result

A summary of the current configuration is shown.

# Show the status of the User ID Service

Use the Configuration Utility to check the status of the User ID Service. In an HA configuration, the status of all the cluster members is shown.

## Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.
- 2) Enter the following command:

```
fuid-cfg status
```

## Result

You are shown detailed information, such as information about the services that run in the User ID Service.

If you have configured HA, you can also see the status of the cluster members. When HA is successfully configured, the value for the `is_available` and `is_live` columns is `true`.

### Related information

[Using the User ID Service and DC Agent in an HA configuration](#) on page 85

# Configure the UID Server

The UID Server is configured during the initial setup, but you can later make changes and modify advanced settings.

The UID Server communicates with the DC Agent, AD and OpenLDAP Servers, the User ID Service Client Product with which the User ID Service has been integrated, and any other source of user or logon data that provides data using the User ID Service API.



### Tip

In many cases, the default option is shown. To use the default option, press **Enter**.

## Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.

- 2) Enter the following command:

```
fuid-cfg uid
```

If you want to configure advanced TLS settings, use the following flag with the command:

```
-a, --advanced
```

- 3) Enter the port that the server uses.  
Use the following format:

```
:<port number>
```

The default port is 5000. By default, the current server IP address is used, but you can also enter another IP address and port.

- 4) If you used the advanced flag, configure the advanced TLS settings.
  - a) Enter the path to the trusted CA file.
  - b) Enter the path to the location of the trusted CA key file.
  - c) Select the cipher suites to use.  
Use the arrow keys to browse the list, press **Space** to make your selections, then press **Enter** to finish making your selection.
  - d) Select the minimum TLS version to use.  
Use the arrow keys to browse the list, then press **Enter** to make your selection.
- 5) When prompted to restart the associated service, enter **Y**.

## Show the UID Server configuration

Use the Configuration Utility to show the current configuration.

### Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.
- 2) Enter the following command:

```
fuid-cfg uid show
```

### Result

A summary of the current configuration is shown.

# Using the User ID Service API

### Contents

- [Overview to using the User ID Service API](#) on page 35
- [Add additional API users](#) on page 35
- [Delete an API user](#) on page 36
- [Show all API users](#) on page 36

The User ID Service API can be used to add, modify, and delete data in the User ID Service CockroachDB database.

## Overview to using the User ID Service API

To interact with or to populate the User ID Service database, you must create an API user for basic authentication.

To use the DC Agent, you must create an API user that the DC Agent uses to interact with the User ID Service.

In an HA configuration, the list of API users is synchronized between cluster members. For more information, see the *Forcepoint User ID Service API User Guide*.

### Related tasks

[Configure User ID Service credentials for the DC Agent](#) on page 77

## Add additional API users

After the initial setup of the User ID Service, you can use the Configuration Utility to add additional API users.

### Steps

1) Log on to the server as root.  
You can also use `sudo` when you enter commands.

2) Enter the following command:

```
fuid-cfg api add-user
```

3) Enter a user name for the API user.

- 4) Enter a password for the API user.

## Result

The API user is added to the configuration.

# Delete an API user

---

If you no longer need an API user, use the Configuration Utility to delete the API user.

## Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.

- 2) Enter the following command:

```
fuid-cfg api del-user
```

- 3) Select the API user to delete.  
Use the arrow keys to browse the list, then press **Enter** to make your selection.
- 4) When prompted to confirm your action, enter `Y`.

## Result

The API user is deleted from the configuration.

# Show all API users

---

Use the Configuration Utility to show all the API users that have been configured.

## Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.

- 2) Enter the following command:

```
fuid-cfg api show
```

## Result

A list of API users is shown.

## Chapter 6

# Configuring LDAP servers

### Contents

- Add an Active Directory server on page 37
- Add OpenLDAP server on page 39
- Configure advanced TLS settings on page 40
- Configure advanced Active Directory server settings on page 41
- Configure advanced OpenLDAP server settings on page 42
- Test the connection to LDAP servers on page 42
- Configure global LDAP settings on page 43
- Show the LDAP server configurations on page 44
- Modify an LDAP server on page 44
- Remove an LDAP server on page 45
- Configure the LDAP server synchronization frequency on page 45
- Synchronize with the LDAP server manually on page 47
- Unlock an LDAP server on page 47

Use the Configuration Utility to add, modify, or remove LDAP servers that represent AD or OpenLDAP servers.

## Add an Active Directory server

Use the Configuration Utility to add an Active Directory server from which the User ID Service receives data about groups and users.

You can add an LDAP server during the initial setup, and later add additional LDAP servers.



### Tip

In many cases, the default option is shown. To use the default option, press **Enter**.



### Tip

Press **Ctrl+C** to cancel an action.

### Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.

- 2) Enter the following command:

```
fuid-cfg ldap add
```

- 3) Enter the IP address of the AD Server.
- 4) Enter the port that the AD Server listens on.  
The default port is 3268. For a secure LDAP (LDAPS) server, use port 3269.
- 5) Enter the base distinguished names (DN) for LDAP search.  
You can enter multiple base DNs on separate lines. Press **Enter** twice after you have entered the DNs.
- 6) Enter the user name of the account used to access the LDAP server.  
Enter the name in distinguished format. For example:
- ```
cn=administrator,cn=users,dc=example,dc=com
```
- 7) Enter the password of the account used to access the LDAP server.
- 8) To synchronize only users that have an email address, enter **Y**. Otherwise, enter **N**.  
You can use this option to, for example, avoid synchronizing service accounts that do not have email addresses associated with them.
- 9) To enable support for nested groups, enter **Y**. Otherwise, enter **N**.  
If there is a large number of groups per user definition, nested groups can have an impact on performance.
- 10) To enable TLS encryption for the connection to the server, enter **Y**. Otherwise, enter **N**.
- 11) If you enabled TLS encryption, and want to enable strict TLS verification, enter **Y**. Otherwise, enter **N**.  
When enabled, you must have a CA installed that matches the CA on the AD Server. The CA and host name must match.
- 12) To configure advanced TLS or LDAP server settings, enter **Y**. Otherwise, enter **N**.

## Next steps

If you selected to configure advanced settings, continue the configuration in the Configuration Utility.

Otherwise, the LDAP server is added to the configuration.

The User ID Service synchronizes with the LDAP server, populating the CockroachDB database.

### Related concepts

[Best practices for LDAP servers configuration](#) on page 8

# Add OpenLDAP server

Use the Configuration Utility to add an OpenLDAP server from which the User ID Service receives data about groups and users.

You can add an LDAP server during the initial setup, and later add additional LDAP servers.

## Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.
- 2) Enter the following command:

```
fuid-cfg ldap add
```
- 3) Enter the IP address of OpenLDAP Server.
- 4) Enter the port that the OpenLDAP Server listens on.  
The default port is 389. For a secure LDAP (LDAPS) server, use port 636.
- 5) Enter the base distinguished names (DN) for LDAP search.  
You can enter multiple base DNs on separate lines. Press **Enter** twice after you have entered the DNs.
- 6) Enter the user name of the account used to access the LDAP server.  
Enter the name in the following sample format:

```
cn=administrator,cn=users,dc=example,dc=com
```
- 7) Enter the password of the account used to access the LDAP server.
- 8) To synchronize only users that have an email address, enter **Y**, else enter **N**.  
You can use this option to avoid synchronizing service accounts that do not have email addresses associated with them.
- 9) To enable TLS encryption for connecting to the server, enter **Y**, else enter **N**.
- 10) To enable strict TLS verification after enabling TLS encryption, enter **Y**, else enter **N**.  
When enabled, you must have a CA installed that matches the CA on the OpenLDAP Server. The CA and host name must match.
- 11) To configure advanced TLS or LDAP server settings, enter **Y**, else, enter **N**.

# Configure advanced TLS settings

If you selected to configure advanced settings, continue the configuration in the Configuration Utility.



## Tip

In many cases, the default option is shown. To use the default option, press **Enter**.

## Steps

- 1) Enter the path to the location of the trusted CA file.  
The default location is the system CA store.
- 2) Select the cipher suites to use.  
Use the arrow keys to browse the list, press **Space** to make your selections, then press **Enter** to finish making your selection. To use the default list of ciphers, press **Enter**.  
The User ID Service uses the Go Language TLS module. TLS 1.3 algorithms are used first, then TLS 1.2 algorithms. For more information, see <https://golang.org/pkg/crypto/tls/>.
- 3) Select the minimum TLS version to use.  
Use the arrow keys to browse the list, then press **Enter** to make your selection.
- 4) To enable revocation checking, enter **Y**. Otherwise, enter **N**.  
When you enable revocation checking, all server certificates are checked against denied certificate revocation lists (CRL) and online certificate status protocol (OCSP). Revocation information must be included in the certificate. You cannot use CRLs for checking LDAP URLs. Only HTTP URLs are supported.
- 5) If you enabled revocation checking, select the default action if a certificate has been revoked.  
Use the arrow keys to browse the list, then press **Enter** to make your selection.
- 6) To enable peer identity checking, enter **Y**. Otherwise, enter **N**.
- 7) If you enabled peer identity checking, select the peer certificate attribute to match against.  
Use the arrow keys to browse the list, then press **Enter** to make your selection.
- 8) If you enabled peer identity checking, enter the value for the peer certificate attribute to match against.

## Next steps

Configure the advanced LDAP server settings in the Configuration Utility.



# Configure advanced Active Directory server settings

If you selected to configure advanced settings, continue the configuration in the Configuration Utility.



## Tip

In many cases, the default option is shown. To use the default option, press **Enter**.

We recommend you change the defaults only if you are familiar with the advanced configuration of LDAP servers.

## Steps

- 1) Enter the SID attribute of the LDAP server.  
The default value is `objectSid`.
- 2) Enter the GUID attribute of the LDAP server.  
The default value is `objectGUID`.
- 3) Enter the SAM account name of the LDAP server.  
The default value is `sAMAccountName`.
- 4) Enter the MemberOf attribute of the LDAP server.  
The default value is `memberOf`.
- 5) Enter the NTLM user name of the LDAP server.  
The default value is `NTLMIdentity`.
- 6) Enter the Mail attribute of the LDAP server.  
The default value is `mail`.
- 7) Enter the User Filter attribute of the LDAP server.  
The default value is `(&(objectCategory=person)(objectclass=user))`.
- 8) Enter the Group Filter attribute of the LDAP server.  
The default value is `(&(objectCategory=group)(objectclass=group))`.
- 9) Enter the size of the LDAP search page for the LDAP server.  
The default value is `1000`.

## Result

The User ID Service synchronizes with the LDAP server, populating the CockroachDB database.

# Configure advanced OpenLDAP server settings

If you selected to configure advanced settings, continue the configuration in the Configuration Utility.



## Tip

In many cases, the default option is shown. To use the default option, press **Enter**.

We recommend you change the defaults only if you are familiar with the advanced configuration of LDAP servers.

## Steps

- 1) Enter the Primary User Attribute. This value represents a unique user attribute in the LDAP definition.  
The default value is `cn`.
- 2) Enter the Primary Group Attribute. This value represents a unique group attribute in the LDAP definition.  
The default value is `cn`.
- 3) Enter the Mail attribute of the LDAP server.  
The default value is `mail`.
- 4) Enter the User Filter attribute of the LDAP server.  
The default value is:  
`((|(objectclass=inetOrgPerson)(objectclass=person) (objectclass=organizationalPerson)))`
- 5) Enter the Group Filter attribute of the LDAP server.  
The default value is:  
`((|(objectclass=groupOfNames)(objectclass=country) (objectclass=organization) (objectclass=organizationalUnit)))`
- 6) Enter the size of the LDAP search page for the LDAP server.  
The default value is 1000.

## Test the connection to LDAP servers

Use the Configuration Utility to test that the connection to all configured LDAP servers works and that the credentials are correct.



## Tip

Press **Ctrl+C** to cancel an action.

## Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.
- 2) Enter the following command:

```
fuid-cfg ldap test
```

## Result

If the User ID Service successfully connects with the specified credentials, the Configuration Utility confirms that the connection was successful.

# Configure global LDAP settings

To configure global LDAP settings:

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.
  - 2) Enter the following command:
- ```
fuid-cfg ldap settings
```
- 3) To enable support for nested groups, enter Y. Otherwise, enter N.  
If there is a large number of groups per user definition, nested groups can have an impact on performance.
  - 4) If you want to configure LDAP user and group filters, enter Y. Otherwise, enter

## Configure LDAP Filters

You can apply LDAP filters after fetching LDAP data. LDAP filters let you to configure regular expressions to include and exclude users and groups. LDAP filter are compared against the user or group DN LDAP attribute. Include regular expressions are applied before exclude regular expressions:

- Select if you want to modify the include users regular expressions.
- Select if you want to modify the exclude users regular expressions.
- Select if you want to modify the include groups regular expressions.
- Select if you want to modify the exclude groups regular expressions.

# Show the LDAP server configurations

Use the Configuration Utility to show all the configured LDAP servers and the configuration details.



## Tip

Press **Ctrl+C** to cancel an action.

## Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.

- 2) Enter the following command:

```
fuid-cfg ldap show
```

## Result

The LDAP server configuration information is shown.

# Modify an LDAP server

Use the Configuration Utility to modify the settings for an LDAP server.



## Tip

Press **Ctrl+C** to cancel an action.

## Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.

- 2) Enter the following command:

```
fuid-cfg ldap modify
```

- 3) Select the LDAP server that you want to modify.
- 4) Follow the same steps as when you added the LDAP server.
- 5) When prompted to confirm your action, enter `Y`.

## Result

The LDAP server configuration is updated.

### Related tasks

Add an Active Directory server on page 37

## Remove an LDAP server

Use the Configuration Utility to remove an LDAP server from the configuration.



### Tip

Press **Ctrl+C** to cancel an action.

### Steps

1) Log on to the server as root.  
You can also use `sudo` when you enter commands.

2) Enter the following command:

```
fuid-cfg ldap delete
```

3) Select the LDAP server that you want to delete.

4) When prompted to confirm your action, enter `Y`.

### Result

The LDAP server is deleted from the configuration.

User definitions from the AD domain that have previously been added to the CockroachDB database are not removed.

## Configure the LDAP server synchronization frequency

You can configure how frequently the User ID Service synchronizes data about users and groups with AD and OpenLDAP servers. You can set the User ID Service to synchronize at regular intervals or once a day at a set time.



### Important

Synchronizing with large AD and OpenLDAP servers too frequently can cause performance issues. We recommend that you do not synchronize more frequently than every 15 minutes.



### Tip

Press **Ctrl+C** to cancel an action.

## Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.

- 2) Enter the following command:

```
fuid-cfg ldap sync
```

- 3) Select whether to synchronize at regular intervals or at a specific time each day.
- 4) If you chose to synchronize at regular intervals, enter the frequency in hours and minutes.  
Use the format:

```
<hour>h<minutes>m
```

or

```
<minutes>m
```

Examples:

```
48h
```

```
6h30m
```

```
45m
```

- 5) If you chose to synchronize once a day at a set time, enter the time.  
Use the format:

```
HH:mm
```

Examples:

```
07:00
```

```
18:30
```

- 6) When prompted to restart the associated service, enter `Y`.

# Synchronize with the LDAP server manually

If the scheduled synchronization is infrequent, you can synchronize with the LDAP server at any time manually if needed.



## Important

Synchronizing with large AD and OpenLDAP servers too frequently can cause performance issues. We recommend that you do not synchronize more frequently than every 15 minutes.

## Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.
- 2) Enter the following command:

```
fuid --sync-ldap
```

## Result

The User ID Service synchronizes with the AD or OpenLDAP server, updating the CockroachDB database.

# Unlock an LDAP server

When the User ID Service synchronizes with an LDAP server, the LDAP update process is locked so that no other LDAP synchronization can occur at the same time.



## Important

It can take double the length of the synchronization frequency time for the lock to be automatically released, especially when synchronizing for the first time. We recommend that you manually unlock the update process only when advised to by Forcepoint support.

## Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.
- 2) Enter the following command:

```
fuid-cfg db unlock
```

## Result

The LDAP update process is unlocked.





## Chapter 7

# Configuring certificates for the User ID Service

### Contents

- Certificates used in the User ID Service on page 49
- Configure LDIF hybrid cloud user synchronization on page 50
- Using externally-signed certificates on page 52
- Create a self-signed certificate on page 56
- View the contents of the installed certificate on page 57
- View the supported TLS versions and cipher suites on page 57

Use the Configuration Utility to configure certificates and security settings for the User ID Service.

## Certificates used in the User ID Service

TLS encryption is automatically enabled for communication between most of the components in the User ID Service.



### Note

If you disable TLS encryption, make sure that communication is routed only over secured networks.

## Communication with external components

For communication between the UID Server and external components, such as the User ID Service Client Product, a self-signed certificate (`server.crt`) and key (`server.key`) are created in the `/etc/fuid` directory during the initial setup of the User ID Service. Rather than using the self-signed certificate, we recommend that you use an externally-signed certificate.

## Communication with the CockroachDB database

A root CA certificate (`ca.crt`) and key (`ca.key`) for the CockroachDB database are created in the `/var/lib/cockroach` directory during the initial setup of the User ID Service. In an HA configuration, you must copy the root CA certificate and key to all cluster members.

For communication between the User ID Service and the CockroachDB database, a client certificate (`client.fuid.crt`) signed by the root CA and a key (`client.fuid.key`) are created in the `/etc/fuid` directory.

Additional certificates and keys for the CockroachDB database are automatically created in the `/var/lib/cockroach` directory and signed by the root CA.

**Note**

We recommend that you do not modify the CockroachDB certificate configuration. For more information, see <https://www.cockroachlabs.com>.

## Communication with LDAPS servers

For secure LDAP (LDAPS), copy and import the certificates from the AD or OpenLDAP servers.

# Configure LDIF hybrid cloud user synchronization

FUID can be configured to generate user and group LDAP LDIF files that are sent to an on premise Forcepoint Security Manager (FSM), using the FSM SyncService. The FSM SyncService then transmits the LDIF data to the Forcepoint Hybrid Cloud, updating the user and group definitions.

LDAP updates results in synchronizations to the SyncService.

Enabling LDIF synchronization:

- Disables nested group lookups.
- Restricts the LDAP synchronization time to no less than 1 hour.
- Removes all existing user data from the database.

Additionally, use of the following API calls is not recommended when LDIF is enabled:

- POST /api/uid/v1.0/user/{Object GUID}
- PUT /api/uid/v1.0/user/{Object GUID}
- DELETE /api/uid/v1.0/user/{Object GUID}
- POST /api/uid/v1.0/user/ntlm-identity/{NetBIOS\Username}
- PUT /api/uid/v1.0/user/ntlm-identity/{NetBIOS\Username}

**Note**

FUID communicates with the Windows SyncService using TCP port 55832. Since FUID is running externally from SyncService, you need to create a Windows firewall rule to allow communication over TCP port 55832.

## Setup LDIF synchronization

- 1) Log on to the server as `root`.  
You can also use `sudo` when you enter commands.
- 2) Enter the following command:

```
fuid-cfg ldif setup
```

- 3) Read and acknowledge the warning presented regarding LDIF setup.
- 4) Set the SyncService IP address. It is recommended to use an IP address for SyncService instead of a host name.
- 5) Set the SyncService Port. The default is 55832.
- 6) Set the SyncService Timeout. The default is 1 hour.
- 7) To configure secure TLS communication with the SyncService select **Y**. Otherwise, select **N**.  
If secure TLS is enabled, you must import the Certificate Authority used to sign SyncService certificates into the local store on the FUID server.
- 8) Set the directory where you will place LDIF files. The default is `/etc/fuid/ldifs`.
- 9) If you want to delete the LDIF files after they are sent to the SyncService, select **Y**. Otherwise, select **N**.
- 10) Set the mail regular expression matching pattern.
- 11) Select the synchronization interval. The minimum synchronization interval is 1 hour.
- 12) Acknowledge the warning about flushing user data.

## Modify LDIF synchronization

---

- 1) Log on to the server as `root`.  
You can also use `sudo` when you enter commands.
- 2) Enter the following command:

```
fuid-cfg ldif modify
```
- 3) Set the SyncService IP address. It is recommended to use an IP address for SyncService instead of a host name.
- 4) Set the SyncService Port. The default is 55832.
- 5) Set the SyncService Timeout. The default is 1 hour.
- 6) To configure secure TLS communication with the SyncService select **Y**. Otherwise, select **N**.  
If secure TLS is enabled, you must import the Certificate Authority used to sign SyncService certificates into the local store on the FUID server.
- 7) Set the directory where you will place LDIF files. The default is `/etc/fuid/ldifs`.
- 8) If you want to delete the LDIF files after they are sent to the SyncService, select **Y**. Otherwise, select **N**.

- 9) Set the mail regular expression matching pattern.
- 10) Select the synchronization interval. The minimum synchronization interval is 2 hour.
- 11) If you want to restart the fuid service, select Y. Otherwise, select N.

## Disable LDIF synchronization

---

- 1) Log on to the server as `root`.  
You can also use `sudo` when you enter commands.
- 2) Enter the following command:  

```
fuid-cfg ldif disable
```
- 3) Confirm you want to disable LDIF hybrid cloud synchronization.
- 4) If you want to restart the fuid service, select `Y`. Otherwise, select `N`.

## Show LDIF synchronization configuration

---

- 1) Log on to the server as `root`.  
You can also use `sudo` when you enter commands.
- 2) Enter the following command:

```
fuid-cfg ldif show
```

# Using externally-signed certificates

---

There are two ways to use an externally-signed certificate to secure communications between User ID Service and external components: you can either import an existing certificate and key pair, or create a certificate request and sign it externally.

# Import a certificate and key pair

Use the Configuration Utility to import an existing certificate and key pair to the User ID Service configuration.

## Before you begin

Create a certificate and key pair externally. The certificate and key must be in separate files. The certificate can be in PEM or DER format. For ease of use, we recommend using PEM format. The key must be an RSA key. We recommend a key length of 2048 or 4096 bits.



### Important

Import the certificate and key pair only after you have performed the initial setup of the User ID Service. If you run the `fuid-cfg setup` command after you have imported the certificate and key pair, the certificate and key pair is overwritten.



### Tip

Press **Ctrl+C** to cancel an action.

## Steps

- 1) Copy the certificate and key pair to the server on which the User ID Service is installed.
- 2) Log on to the server as root.  
You can also use `sudo` when you enter commands.
- 3) Enter the following command:

```
fuid-cfg tls import-pair -c <path to certificate file> -k <path to key file>
```

- 4) When prompted to restart the associated service, enter `Y`.

## Result

The imported certificate and key pair is added to the User ID Service configuration.

# Create a certificate request and sign it externally

Create a certificate request in the User ID Service, use an external CA to sign the certificate request, then import the signed certificate.

## Create a certificate request

Use the Configuration Utility to create a certificate request for the User ID Service.

When you create a certificate request, the existing certificate and private key are removed. A new key is generated, and the certificate request is generated from the key.



### Tip

Press **Ctrl+C** to cancel an action.

## Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.
- 2) Enter the following command:

```
fuid-cfg tls cert-request
```

To save the certificate request as a file, use the following flag to specify the path and file name:

```
-o, --out [path]
```
- 3) When prompted to confirm your action, enter `Y`.
- 4) Enter the host name of the server to use as the common name in the certificate.  
The Configuration Utility detects the current host name of the server and offers that host name as the default. To use the default option, press **Enter**.
- 5) To specify a subjectAltName for the certificate, enter a comma-separated list of DNS names or IP addresses. This option is useful if multiple User ID Service Client Products need to communicate with the User ID Service, and specific peer identity values are required. To skip this step, press **Enter**.
- 6) To configure additional attributes for the certificate, enter `Yes`, then configure the attributes.  
To leave an attribute unspecified, press **Enter**.
  - a) Enter a two-letter country code.
  - b) Enter the name of the state or province.
  - c) Enter the name of the locality.
  - d) Enter the name of the organization.

- e) Enter the name of the organizational unit.

## Result

If you did not specify a path and file name, the contents of the certificate request are shown for you to copy.

## Next steps

Sign the certificate request with an external Certificate Authority, then import the signed certificate to the User ID Service configuration.

# Import a signed certificate

Use the Configuration Utility to import a signed certificate in PEM format to the User ID Service configuration.

## Before you begin

Copy the signed certificate to the server on which the User ID Service is installed.



### Tip

Press **Ctrl+C** to cancel an action.

## Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.

- 2) Enter the following command:

```
fuid-cfg tls cert-import
```

If the signed certificate is not in the current directory and named `server.crt`, use the following flag to specify the path and file name:

```
-f, --file [path]
```

- 3) When prompted to restart the associated service, enter `Y`.

## Result

The signed certificate is added to the User ID Service configuration.

# Create a self-signed certificate

A self-signed certificate and private key are automatically created when you perform the initial setup of the User ID Service. Use the Configuration Utility to create a new self-signed certificate and private key for the User ID Service.

When you create a self-signed certificate and private key, the existing certificate and private key are replaced.



## Tip

Press **Ctrl+C** to cancel an action.

## Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.
- 2) Enter the following command:

```
fuid-cfg tls cert-self
```
- 3) When prompted to confirm your action, enter `Y`.
- 4) Enter the host name of the server to use as the common name in the certificate.  
The Configuration Utility detects the current host name of the server and offers that host name as the default. To use the default option, press **Enter**.
- 5) To specify a subjectAltName for the certificate, enter a comma-separated list of DNS names or IP addresses. This option is useful if multiple User ID Service Client Products need to communicate with the User ID Service, and specific peer identity values are required. To skip this step, press **Enter**.
- 6) To configure additional attributes for the certificate, enter `Yes`, then configure the attributes. To leave an attribute unspecified, press **Enter**.
  - a) Enter a two-letter country code.
  - b) Enter the name of the state or province.
  - c) Enter the name of the locality.
  - d) Enter the name of the organization.
  - e) Enter the name of the organizational unit.
- 7) When prompted to restart the associated service, enter `Y`.

## Result

A new self-signed certificate and private key are generated and saved in the `/etc/fuid` directory, and automatically added to the User ID Service configuration.



# View the contents of the installed certificate

---

You can view the contents of the installed certificate in the Configuration Utility.

## Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.
- 2) Enter the following command:

```
fuid-cfg tls cert-show
```

## Result

The contents of the installed certificate are shown.

# View the supported TLS versions and cipher suites

---

Use the Configuration Utility to see what TLS versions and cipher suites are supported.

## Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.
- 2) Enter the following command:

```
fuid-cfg tls info
```

## Result

The supported TLS versions and cipher suites are shown. The User ID Service uses the Go Language TLS module. TLS 1.3 algorithms are used first, then TLS 1.2 algorithms. For more information, see <https://golang.org/pkg/crypto/tls/>.



## Chapter 8

# Configuring the CockroachDB database

### Contents

- Configure the CockroachDB database on page 59
- Modify the expiration time of logon data on page 61
- Query the database for a specific user, IP address, or security identifier on page 62

The CockroachDB database is an SQL database that stores data received through the User ID Service API from the DC Agent, AD and OpenLDAP server, and other sources of user or logon data.

In a high-availability (HA) configuration, the database is synchronized between cluster members. For more information about CockroachDB, go to <https://www.cockroachlabs.com>.

The CockroachDB database is populated through the User ID Service API. Other sources of user or logon data can use the User ID Service API to interact with the database. For more information, see the *Forcepoint User ID Service API User Guide*.

## Configure the CockroachDB database

The CockroachDB database is configured during the initial setup, but you can later modify the configuration.



### Tip

Press **Ctrl+C** to cancel an action.



### Tip

In many cases, the default option is shown. To use the default option, press **Enter**.

### Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.

- 2) Enter the following command:

```
fuid-cfg db
```

- 3) Enter the IP address of the server that the CockroachDB database is installed on.

- 4) If the server is part of a cluster of servers in an HA configuration, enter a comma-separated list of IP addresses that represent the other servers.
- 5) When prompted to restart the associated service, enter **Y**.

## Show the CockroachDB database configuration

Use the Configuration Utility to show the current configuration.

### Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.
- 2) Enter the following command:

```
fuid-cfg db show
```

### Result

A summary of the current configuration is shown.

## Delete all data from the CockroachDB database

If needed, you can delete all data from the CockroachDB database.



#### CAUTION

Only delete the data if instructed to do so by [Forcepoint Customer Hub](#).



#### Important

All User ID Service API users are removed from the configuration.

### Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.
- 2) Enter the following command:

```
fuid-cfg db flush
```

- 3) When prompted to confirm your action, enter **Y**.

## Result

All data from the CockroachDB database is deleted.

# Modify the expiration time of logon data

By default, the mapping between a user and their IP address in the CockroachDB database expires after 6 hours. You can use the Configuration Utility to modify the expiration time.



### Tip

Press **Ctrl+C** to cancel an action.

## Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.

- 2) Enter the following command:

```
fuid-cfg logon [DURATION]
```

Where `[DURATION]` is the length of time. Examples:

```
8h
```

```
4h30m
```

# Show the expiration time of logon data

Use the Configuration Utility to show how long it takes before the mapping between a user and their IP address in the CockroachDB database expires.

## Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.

- 2) Enter the following command:

```
fuid-cfg logon show
```

## Result

The expiration time is shown.

# Query the database for a specific user, IP address, or security identifier

Use the Configuration Utility to check the details of a specific user, IP address, or security identifier (SID).

## Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.

- 2) Enter the following command:

```
fuid-cfg logon query -a [IP address]
```

or

```
fuid-cfg logon query -u [user name]
```

or

```
fuid-cfg logon query -s [SID]
```

Where `[IP address]` is the IP address that you want to query, `[user name]` is the user name that you want to query, or `[SID]` is the SID that you want to query.

## Result

A summary of the information is shown.

## Chapter 9

# Configuring logging for the User ID Service

### Contents

- Select the log level on page 63
- View User ID Service log events on page 65
- Forwarding log data to the SMC on page 65

You can set the log level, view the logs for the User ID Service, and forward log data to the SMC.

## Select the log level

To configure how much log data is generated, select the log level in the Configuration Utility. By default the log level is INFO. Information that is generally useful is logged.



### Tip

Press **Ctrl+C** to cancel an action.

### Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.
- 2) Enter the following command:

```
fuid-cfg log level
```

The current log level is shown.

- 3) Use the arrow keys to browse the list, then press **Enter** to make your selection.  
Select from the following:
  - **FATAL** — Only fatal errors are logged.
  - **ERROR** — Only errors are logged.
  - **WARNING** — Only warnings are logged.
  - **INFO** — Information that is generally useful is logged. This log level is the default log level.
  - **DEBUG** — Information that is useful for support is logged.
  - **TRACE** — All available information is logged.



#### Note

When you select a log level, both the logs of that level and higher are generated.

- 4) When prompted to restart the associated service, enter **Y**.

## Result

Logs of the selected level are generated.

# Show the log level

You can show the current log level in the Configuration Utility.

## Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.
- 2) Enter the following command:

```
fuid-cfg log show
```

## Result

The current log level is shown. The log level is one of the following:

- **FATAL** — Only fatal errors are logged.
- **ERROR** — Only errors are logged.
- **WARNING** — Only warnings are logged.
- **INFO** — Information that is generally useful is logged. This log level is the default log level.
- **DEBUG** — Information that is useful for support is logged.
- **TRACE** — All available information is logged.



#### Note

When you select a log level, both the logs of that level and higher are generated.



# View User ID Service log events

To view log data for the User ID Service or the CockroachDB database, use the standard Linux journal facility.

## Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.
- 2) Enter the following command:

```
journalctl -xeu [service] | less
```

Where `[service]` is `fuid` or `cockroach`.

## Result

The log data is shown in standard journal facility format.

# Forwarding log data to the SMC

You must enable log forwarding in the Configuration Utility, then you must use the Management Client component of the SMC (SMC Management Client) to configure the SMC to receive log data from the User ID Service.

## Enable forwarding log data to the SMC

Use the Configuration Utility to enable log forwarding from the User ID Service to the SMC.



### Tip

Press **Ctrl+C** to cancel an action.

## Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.
- 2) Enter the following command:

```
fuid-cfg log smc-forward
```
- 3) Enter the IP address of the Log Server to which you want to forward log data.
- 4) Enter the syslog port of the Log Server to which you want to forward logs.  
The default port is 5514.

- 5) When prompted to restart the associated service, enter **Y**.

## Next steps

Use the SMC Management Client to configure the SMC to receive log data from the User ID Service.

# Configure the SMC to receive log data

In the SMC Management Client, configure the SMC to receive log data from the User ID Service.



If you use Forcepoint NGFW 6.4 or higher, use a Forcepoint User ID Service element to define the settings for communication between the NGFW Engine and the User ID Service. For more information, see the section about integrating Forcepoint NGFW as the User ID Service Client Product.

If you use Forcepoint NGFW 6.3, use a Host element to define the settings for communication between the NGFW Engine and the User ID Service.

## Create a logging profile

Create a logging profile to define which log data from the User ID Service the SMC receives and how the log data is shown in the SMC Management Client.

**Steps**  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Open the SMC Management Client.
- 2) Select  **Configuration**, then browse to **Monitoring**.
- 3) Browse to **Third-Party Devices > Logging Profiles**.
- 4) Select  **New > Logging Profile**.
- 5) Enter a name for the Logging Profile, then click **OK**.  
The Logging Profile opens for editing. By default, unmatched log events are saved in the "Syslog message field". You can use the default settings in the Logging Profile.
- 6) Close the Logging Profile editor.

## Result

The SMC starts receiving log data from the User ID Service. The log data is shown in the "Syslog message" field in the Logs view of the Management Client.

## Next steps


- If you are using Forcepoint NGFW version 6.4 or higher, configure the monitoring options in the Forcepoint User ID Service element.
- If you are using Forcepoint NGFW version 6.3, create a Host element that represents the User ID Service.


# Enable monitoring in the Forcepoint User ID Service element

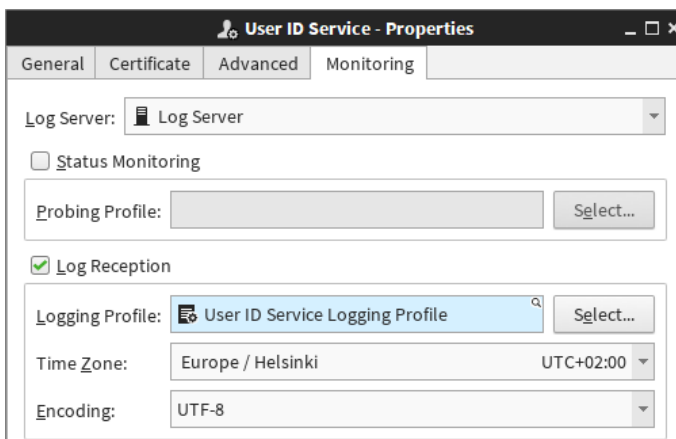
For Forcepoint NGFW version 6.4 or higher, enable monitoring in the properties of the Forcepoint User ID Service element.

## Before you begin

Create a Forcepoint User ID Service element.

**Steps**  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Open the SMC Management Client.
- 2) Select  **Configuration**.
- 3) Browse to **Other Elements > Engine Properties > User Identification Services**.
- 4) Right-click the Forcepoint User ID Service element, then select **Properties**.
- 5) On the **Monitoring** tab, select the Log Server that receives log data from the User ID Service.
- 6) Select **Log Reception**, then select the Logging Profile that you created.



- 7) Click **OK**.
- 8) If there is a Firewall between the User ID Service server and the Log Server, create an Access rule in the Firewall policy to allow communication between the User ID Service server and the Log Server.

## Result


The SMC starts receiving log data from the User ID Service. The log data is shown in the "Syslog message" field in the Logs view of the SMC Management Client.



**Related tasks**

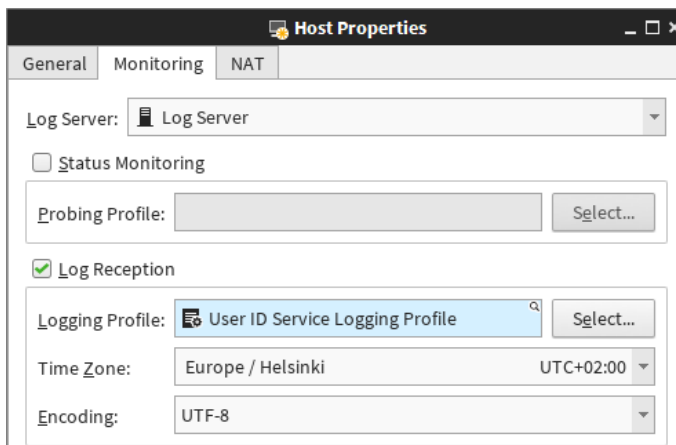
Create a Forcepoint User ID Service element on page 97

## Create a Host element that represents the User ID Service

For Forcepoint NGFW version 6.3, create a Host element that represents the server on which the User ID Service is installed, then enable monitoring.

**Steps**  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Open the SMC Management Client.
- 2) Select  **Configuration**, then browse to **Network Elements**.
- 3) Browse to **Hosts**.
- 4) Select  **New > Host**.
- 5) On the **General** tab, enter a name, then enter the IP address of the User ID Service server.
- 6) On the **Monitoring** tab, select the Log Server that receives log data from the User ID Service.
- 7) Select **Log Reception**, then select the Logging Profile that you created.



- 8) If there is a NAT device between the User ID Service and the Log Server, add NAT definitions as needed on the **NAT** tab.
- 9) Click **OK**.
- 10) If there is a Firewall between the User ID Service server and the Log Server, create an Access rule in the Firewall policy to allow communication between the User ID Service server and the Log Server.

## Result

The SMC starts receiving log data from the User ID Service. The log data is shown in the "Syslog message" field in the Logs view of the SMC Management Client.



# Installing the DC Agent

### Contents

- [Overview to installing the DC Agent on page 71](#)
- [Requirements on page 72](#)
- [Obtaining installation files on page 72](#)
- [Install the DC Agent on page 73](#)

Install the DC Agent on a Windows server that is a Domain member.

## Overview to installing the DC Agent

---

Complete the following high-level steps to install the DC Agent.

- 1) Obtain the installation file.
- 2) Install the DC Agent on a Windows machine that is connected to the domain that you want to monitor. We recommend that you install the DC Agent on a Windows Server.

To use the DC Agent in an HA configuration, you must install and configure the DC Agent on another server. For more information, see the separate section about HA configuration.

### Related concepts

[Overview to configuring HA for the DC Agent on page 91](#)

# Requirements

---

See the [Release Notes](#) for information about hardware and system requirements for the User ID Service and the DC Agent for the Forcepoint User ID Service.

## Obtaining installation files

---

Download the installation files, then check the file integrity.

### Download installation files

---

Download the installation files from the Forcepoint website.

- The User ID Service installer is provided as a .run file.
- The DC Agent installer is provided as a .exe file.

#### Steps

- 1) Go to <https://support.forcepoint.com/Downloads>.
- 2) Enter your license code or log on using an existing user account.
- 3) Click **All Downloads**, then browse to the **Network Security** section.
- 4) Under **User ID Service**, select **All versions**.
- 5) Download the installers for the version that you want to install.



#### Important

Download the same version of the User ID Service and DC Agent installers.

## Check the file integrity

---

Before running the installers, check that the installer files have not become corrupt or been changed. Using corrupt files might cause problems at any stage of the installation and use of the system.

#### Steps

- 1) Look up the correct checksum in the [Release Notes](#) or on the Downloads page at <https://support.forcepoint.com/Downloads>.
- 2) Open a command prompt, then go to the directory where you saved the installer file.



- 3) Generate a checksum of the file, where `<filename>` is the name of the installation file.  
From a Linux command prompt, enter:

```
sha256sum <filename>
```

From a Windows PowerShell prompt, enter:

```
Get-FileHash <filename>
```

- 4) Verify that the checksum matches the checksum listed in the Release Notes or on the Downloads page.



#### CAUTION

Do not use files that have invalid checksums. If downloading the files again does not help, contact [Forcepoint Customer Hub](#).

## Install the DC Agent

Use the installation file to install the DC Agent.



#### Note

Do not install the DC Agent on an AD Server or Exchange Server.

The DC Agent must be able to communicate with the AD domain from which it receives data about users and their IP addresses.



#### Note

If Microsoft .Net 4.8 or higher is not already installed on the Windows Server, the bundled Microsoft .Net 4.8 is installed when you install the DC Agent. You are prompted to accept the license terms and install the software.



#### Important

Do not install the DC Agent for the Forcepoint User ID Service and the DC Agent for Forcepoint Web Security on the same server.

### Steps

- 1) Log on to the Windows server using credentials that allow you to install software.
- 2) Browse to the directory where you stored the installer, then double-click the .exe file.
- 3) To start the installation, click **Next**.
- 4) Read the end-user license agreement, select **I accept the terms in the License Agreement**, then click **Next**.
- 5) Click **Install**.

6) When the installation has completed, click **Finish**.

## Result

The DC Agent is installed in the `C:\Program Files\Forcepoint\DCAgent` directory.

## Next steps

Configure the DC Agent.

### Related information

[Configuring the DC Agent on page 75](#)

# Configuring the DC Agent

### Contents

- Overview to configuring the DC Agent on page 75
- Configure the User ID Service details on page 76
- Configure which Domain Controllers and Exchange Servers to poll on page 76
- Configure User ID Service credentials for the DC Agent on page 77
- TLS certificates for the DC Agent on page 78
- Modify the DC Agent service properties on page 79
- Configuring advanced options on page 80
- Troubleshooting the DC Agent on page 83

After installing the DC Agent, there are several configuration tasks that you must perform.

## Overview to configuring the DC Agent

The configuration of DC Agent consists of these high-level steps.

- 1) Add the address of the User ID Service to the DC Agent configuration.
- 2) Configure which Domain Controllers and Exchange Servers the DC Agent polls.
- 3) Configure credentials for authenticating with the User ID Service.
- 4) Configure TLS certificates.
- 5) Modify the DC Agent service properties to use an account that has read permissions to the Domain Controller and Exchange Server event logs.
- 6) (Optional) Configure advanced DC Agent options.

To use the User ID Service in an HA configuration, install and configure the DC Agent on another server. For more information, see the separate section about HA configuration.

### Related information

Using the User ID Service and DC Agent in an HA configuration on page 85

# Configure the User ID Service details

You must add the address of the User ID Service to the DC Agent configuration.

## Steps

- 1) Log on to the Windows server using administrator credentials.
- 2) Browse to the `C:\Program Files\Forcepoint\DCAgent` directory.
- 3) Open the file `config.json` with a text editor such as Notepad.
- 4) In the `fuid_servers` section, replace the placeholder `https://localhost:5000` address with the address and port of the server that you installed the User ID Service on.

Example:

```
"fuid_servers": [  
  "https://10.10.10.1:5000"  
],
```

In an HA configuration, add each cluster member address on a separate line, separated by a comma.

- 5) Save the file.
- 6) Use the Windows Services tool to restart the DC Agent service.

### Related tasks

[Enable HA for the DC Agent on page 91](#)

# Configure which Domain Controllers and Exchange Servers to poll

In some network environments, Domain Controllers might be automatically discovered and added to the DC Agent configuration. You must manually configure which Exchange Servers the DC Agent polls.



### Important

Events with ID 4768 must be enabled on the Domain Controller from which the DC Agent receives data. For more information, see Knowledge Base article [16421](#).

We recommend that you poll Domain Controllers that host the Active Directory Global Catalog.

## Steps

- 1) Log on to the Windows server using administrator credentials.

- 2) Browse to the `C:\Program Files\Forcepoint\DCAgent` directory.
- 3) Open the file `config.json` with a text editor such as Notepad.
- 4) In the `subscribers` section, add entries for the Domain Controllers and Exchange Servers that you want the DC Agent to poll.

Example:

```
{
  "target": "dc1.corp.com",
  "type": 0,
  "enabled": true
},
```

For the `target` parameter, enter the IP address or DNS name of a Domain Controller or Exchange Server.



#### Note

The DC Agent host must be able to resolve the IP addresses of the AD Servers from the DNS names used.

For the `type` parameter, enter either:

- `0` to receive regular logon events (Event ID 4768)
- `1` to receive Exchange Server logon events or successfully authenticated logon events (Event ID 4624)

For the `enabled` parameter, enter `true`. To disable polling for a specific entry, change the value to `false`.

Instead of disabling the polling for an entry, you can also remove the entry. If Domain Controllers are automatically detected in your network environment, to prevent the entry being automatically re-added, disable the domain discovery feature.

- 5) Save the file.
- 6) Use the Windows Services tool to restart the DC Agent service.

#### Related tasks

[Disable domain discovery on page 82](#)

## Configure User ID Service credentials for the DC Agent

You must use User ID Service API user credentials for basic authentication with the User ID Service.

### Before you begin

Create an API user in the User ID Service Configuration Utility.

Credentials are loaded from the personal credential store of the Windows user account that is logged on. The easiest way to add the credentials to the credential store is to use the Microsoft `cmdkey.exe` utility.

## Steps

- 1) Log on to the Windows server using administrator credentials.
- 2) Open a command line prompt using the credentials of the user account that uses the DC Agent.
  - a) In the Windows Start menu, type `cmd`.
  - b) Right-click **Command Prompt**, then select **Run as different user**.
  - c) Run Command Prompt as the same user that uses the DC Agent.
- 3) Use `cmdkey.exe` to enter the User ID Service API user credentials.

Enter the following command:

```
cmdkey.exe /generic:<User ID Service address and port> /user:<user> /pass:<password>
```

The User ID Service address must exactly match the address used in the `config.json` file.

Example:

```
cmdkey.exe /generic:https://10.10.10.1:5000 /user:api_user_1 /pass:api_pass_1
```

You can also provide the argument `/pass:` without the password, to be prompted to enter the password.

## Next steps

In an HA configuration of the DC Agent, add the credentials to each instance of the DC Agent.

### Related tasks

[Add additional API users on page 35](#)

### Related information

[Using the User ID Service and DC Agent in an HA configuration on page 85](#)

# TLS certificates for the DC Agent

Communication between the DC Agent and the User ID Service is secured using TLS.

Certificates are loaded from the Windows certificate store. Add the certificates to the store of the computer that the DC Agent is installed on, not the store for a local account. This store is typically named “Local Machine” or “Manage computer certificates”.

You can use the self-signed certificates that are automatically generated in the User ID Service configuration, but you must make sure that the `SubjectAltName` includes a DNS name or IP address.

## Disable TLS verification

---

If you do not want to secure communications using TLS, you can disable the TLS verification.

### Steps

- 1) Log on to the Windows server using administrator credentials.
- 2) Use the Windows Services tool to stop the DC Agent service.
- 3) Browse to the `C:\Program Files\Forcepoint\DCAgent` directory.
- 4) Open the file `config.json` with a text editor such as Notepad.
- 5) Change the value of the `ssl_verify` parameter to `false`.

```
"ssl_verify": false,
```

- 6) Save the file.
- 7) Use the Windows Services tool to restart the DC Agent service.

## Modify the DC Agent service properties

---

You must modify the DC Agent service to use an account that has read permissions to the Domain Controller and Exchange Server event logs.

### Steps

- 1) Log on to the Windows server using administrator credentials.
- 2) Use the Windows Services tool to stop the DC Agent service.
- 3) Modify the DC Agent service properties.
  - a) Right-click the DC Agent service, then select **Properties**.
  - b) On the **Log On** tab, select a suitable account for the DC Agent service to use.  
The DC Agent service must use a domain account that is in the Event Log Readers group.
- 4) If the DC Agent service does not run using an account that has administrator permissions, add permissions for the DC Agent service to write data to the installation directory.
  - a) Go to the `C:\Program Files\Forcepoint\DCAgent` directory.
  - b) Right-click the directory, then select **Properties**.

- c) On the **Security** tab, select **Full control** as the permissions, then click **OK**.

## Configuring advanced options

You can configure advanced options in the `config.json` and `ignore.txt` files.

### Ignore specified users, IP addresses, or host names

You can configure the DC Agent to ignore specified users or users from specific servers. You can also configure the DC Agent to ignore specific IP addresses, IP address ranges, or host names.

Ignoring users, IP addresses, or host names can be useful, for example, if you want to ignore the IP addresses of multi-user servers, such as terminal servers or file servers.



#### Important

Do not edit or remove the following entries that are included by default: `local service`, `network service`, and `anonymous logon`

The syntax is the following:

```
user<TAB>destination
```

For `user`, enter the user name. To ignore all users, use the wildcard asterisk (\*).

For `destination`, enter one of the following:

- IP Address (Example: `192.168.0.1`)
- IP address range (Example: `192.168.0.1-192.168.0.254`)
- CIDR (Example: `192.168.0.0/24`)
- Host name (Example: `DESKTOP-NAME`)  
The host name must be resolvable by DNS.
- Wildcard to ignore all addresses and host names (Example: `*`)

### Steps

- 1) Log on to the Windows server using administrator credentials.
- 2) Browse to the `C:\Program Files\Forcepoint\DCAgent` directory.
- 3) Open the file `ignore.txt` with a text editor such as Notepad.



- 4) Add each entry on a separate line.

See the following examples.

To ignore the user name `user1` on any machine, enter the following:

```
user1 *
```

To ignore the user `user1` on the machine `DESKTOP-NAME`, enter the following:

```
user1 DESKTOP-NAME
```

To ignore all user names on a specified machine, IP address, or IP address range, enter:

```
* DESKTOP-NAME
* 10.209.34.56
* 10.203.34.1-10.203.34.255
```

The DC Agent ignores the logon events for the machine `DESKTOP-NAME`, the IP address `10.209.34.56`, and the IP address range `10.203.34.1-10.203.34.255`.

- 5) Save the file.
- 6) Use the Windows Services tool to restart the DC Agent service.

## Send logon events from service accounts

By default, the DC Agent does not send data about logon events from service accounts, but if you want the DC Agent to send data about logon events from all accounts, you can configure the DC Agent to do this.

Service accounts are typically identified by the use of a dollar sign (\$) at the beginning of the account name. Computer names can also include a dollar sign at the end of the name.

### Steps

- 1) Log on to the Windows server using administrator credentials.
- 2) Browse to the `C:\Program Files\Forcepoint\DCAgent` directory.
- 3) Open the file `config.json` with a text editor such as Notepad.
- 4) Change the value of the `ignore_dollar_signs` parameter to `false`.

```
"ignore_dollar_signs": false,
```

- 5) Save the file.
- 6) Use the Windows Services tool to restart the DC Agent service.

## Disable domain discovery

---

The Domain Controllers from which the DC Agent polls data about users and IP addresses are automatically added to the DC Agent config.json file when the DC Agent starts. You can disable the automatic domain discovery after all the Domain Controllers have been added to the DC Agent configuration.

### Steps

- 1) Log on to the Windows server using administrator credentials.
- 2) Browse to the `C:\Program Files\Forcepoint\DCAgent` directory.
- 3) Open the file `config.json` with a text editor such as Notepad.
- 4) Change the value of the `domain_discovery` parameter to `false`.

```
"domain_discovery": false,
```

- 5) Save the file.
- 6) Use the Windows Services tool to restart the DC Agent service.

## Enable repeat user login cache

---

The repeat user login cache monitors logins for all IP addresses and ignores repeated logins for specified amount of time. Additionally, it can be used to ignore repeat logins of multiple users on the same IP over a time frame.

To enable repeat user login cache:

### Steps

- 1) Log on to the Windows server using administrator credentials.
- 2) Browse to the `C:\Program Files\Forcepoint\DCAgent` directory.
- 3) Open the file `config.json` in a text editor such as notepad.

4) Change the following configuration values:

```
"cache_size": 128,  
"cache_expiration": 600,  
"ignore_user_limit": 2,  
"ignore_duplicate_login_timeout": 60,
```

- `cache_size` is the maximum size in MB the cache can allocate. The cache is enabled if the value is greater than 0. To disable the cache, set the value to 0.
- `cache_expiration` is a cleanup timeout in seconds for entries in the cache, if left unused.
- `ignore_user_limit` is the maximum number of users disregarded, responsible for repeatedly logging into the same address.
- `ignore_duplicate_login_timeout` is the time in seconds where logins to the same address are ignored.

5) Save the file.

6) Use the Windows Services tool to restart the DC Agent service.

## Troubleshooting the DC Agent

To troubleshoot the DC Agent, there are a few steps that you can take.

### Check the status of the DC Agent process or service

You can use standard Windows tools to monitor the DC Agent.

To check if the DC Agent process is running, open the Windows Task Manager.

To start or stop the DC Agent service, open the Windows Services tool, locate the DC Agent service, then start or stop the service.

### DC Agent log data events

Log data for the DC Agent can be viewed in the standard Windows Event Viewer under **Applications and Services Logs > DC Agent**.



**Tip**

To increase the log file size, open Event Viewer, right-click DC Agent, select **Properties**, then modify the maximum log size.

Events are tagged with an Event ID.



# Using the User ID Service and DC Agent in an HA configuration

### Contents

- Introduction to using an HA configuration on page 85
- Overview to configuring HA for the User ID Service on page 86
- Overview to configuring HA for the DC Agent on page 91

You can use both the User ID Service and the DC Agent in an HA configuration to increase redundancy.

## Introduction to using an HA configuration

In an HA configuration, the User ID Service is installed on an odd number of servers. The CockroachDB database is synchronized between the cluster members.



### Important

We recommend that all members in a cluster are located close enough to each other that there is little latency.

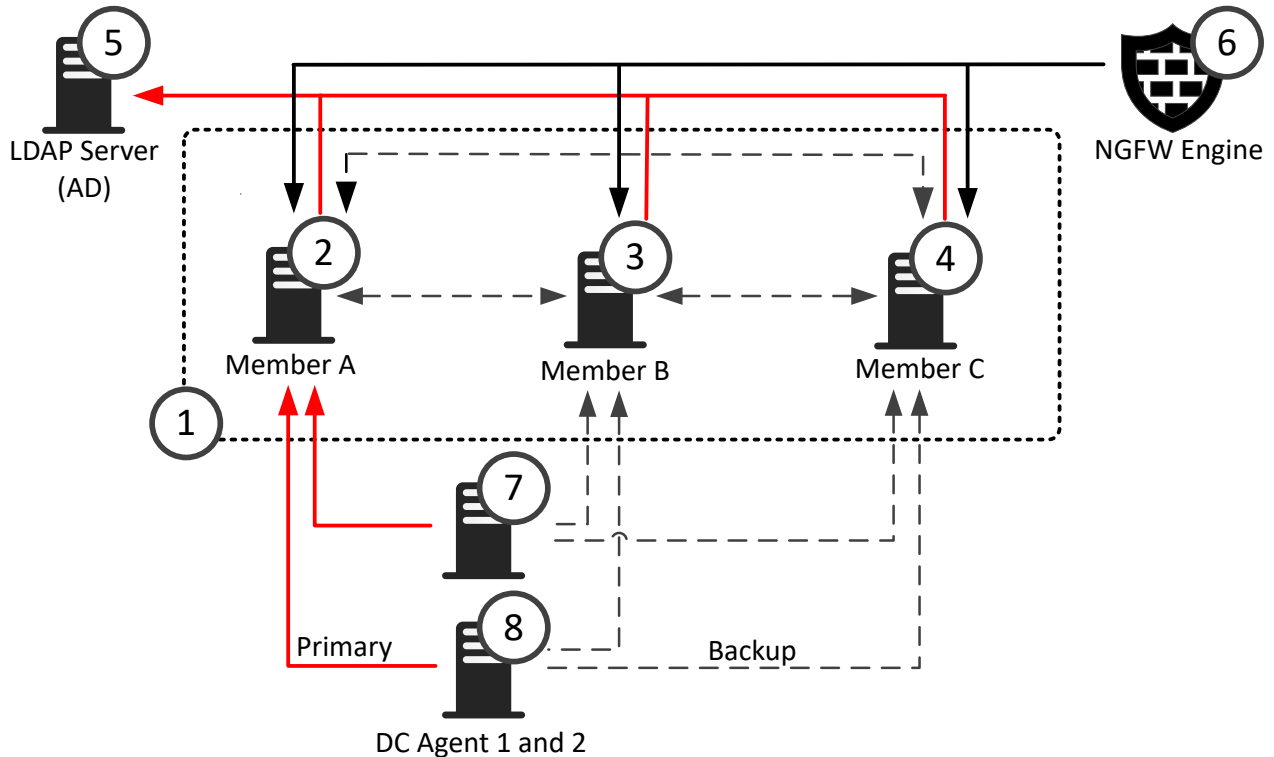
To configure HA for the DC Agent, do one of or both of the following:

- Install more than one instance of the DC Agent on separate servers.
- Add all the User ID Service cluster members to the DC Agent configuration.

For optimal high availability, we recommend that you install the User ID Service in an HA configuration, install multiple instances of the DC Agent, then add all the User ID Service cluster members to the configuration of all the DC Agent instances.

## Example HA configuration

In this example, the Forcepoint NGFW is the User ID Service Client Product.



- 1 The User ID Service is installed on three servers in an HA configuration.
- 2-4 The CockroachDB database that stores data about groups, users, and associated IP addresses is synchronized between all three cluster members.
- 5 The LDAP server that represents the AD Server with which all the cluster members periodically synchronize to update data about users and groups.
- 6 The User ID Service Client Product, in this example, Forcepoint NGFW, can poll data about groups, users, and associated IP addresses from all three cluster members, but only polls one member at a time.
- 7-8 Two instances of the DC Agent are installed on separate servers. Both instances of the DC Agent send data about users and associate IP addresses to a cluster member.  
You can add all the cluster members to the configuration of each DC Agent. If a cluster member becomes unavailable, the DC Agent sends the data to another cluster member.

## Overview to configuring HA for the User ID Service

You must complete the following steps to configure HA for the User ID Service.

- 1) Install the User ID Service on the initial member of the cluster, then perform the initial setup.
- 2) Install the User ID Service on the additional members of the cluster.

- 3) Copy required certificates from the initial cluster member to the additional members of the cluster.
- 4) Perform the initial setup on the additional members of the cluster.
- 5) Check the status of the User ID Service to make sure that all cluster members are available.
- 6) In the User ID Service Client Product that receives data from the User ID Service, configure the settings for the User ID Service.  
If the User ID Service Client Product is the Forcepoint NGFW, enter the IP addresses of all cluster members in the Forcepoint User ID Service element. For more information, see the *Forcepoint Next Generation Firewall Product Guide*.
- 7) Verify that the User ID Service Client Product is receiving data from a cluster member.

## Enable HA on the initial cluster member

Perform the initial setup on the first server that you installed the User ID Service on.

### Before you begin

- Install the User ID Service on the server.
- Configure the host firewall to allow communication between cluster members.



#### Tip

Press **Ctrl+C** to cancel an action.

### Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.
- 2) Enter the following command:

```
fuid-cfg setup
```
- 3) If you want to upgrade from a detected legacy (1.x) installation, enter **Y**. Otherwise, enter **N**.  
If you chose to upgrade, do the following:
  - a) To copy the LDAP server configuration from the legacy installation, enter **Y**. Otherwise, enter **N**.
  - b) If you chose to copy the LDAP server configuration, enter the passwords for the LDAP servers.
  - c) To uninstall the legacy installation, enter **Y**. Otherwise, enter **N**.

- d) To create a backup file of the legacy installation configuration, enter `Y`. Otherwise, enter `N`.  
See the info messages on the command line to see where the backup file is stored.

If an HA configuration is detected, the cluster information and associated certificates are migrated.

- 4) Select **Initial cluster node** as the role of the node.

## Next steps

- 1) Continue performing the initial setup on the initial cluster member.
- 2) Perform the initial setup on the additional cluster members to enable HA.

### Related tasks

[Configure the host firewall](#) on page 15

[Install the User ID Service](#) on page 17

[Start the initial setup](#) on page 19

# Enable HA on an additional cluster member

Perform the initial setup on the additional servers that you installed the User ID Service on.

## Before you begin

- Install the User ID Service and perform the initial setup on the initial cluster member.
- Install the User ID Service on the current server which you are setting up as an additional cluster member.



### CAUTION

The configuration on all cluster members must be exactly the same.



### CAUTION

Use NTP or another suitable protocol to synchronize the time between the servers.



### Tip

Press **Ctrl+C** to cancel an action.



## Steps

- 1) Copy the CockroachDB certificates from the server where you installed the initial cluster member.
  - a) Copy the following files to the same folder on the server where you installed the additional cluster member.

```
/var/lib/cockroach/certs/ca.crt  
/var/lib/cockroach/my-safe-directory/ca.key
```

- b) Apply the correct permissions for the certificate files.  
Enter the following commands:

```
sudo chmod 644 /var/lib/cockroach/certs/ca.crt  
sudo chmod 600 /var/lib/cockroach/my-safe-directory/ca.key
```

- c) Apply the correct ownership for the certificate files.  
Enter the following commands:

```
sudo chown cockroach:cockroach /var/lib/cockroach/certs/ca.crt  
sudo chown cockroach:cockroach /var/lib/cockroach/my-safe-directory/ca.key
```

- 2) Log on to the server as root.  
You can also use `sudo` when you enter commands.

- 3) Enter the following command:

```
fuid-cfg setup
```

- 4) If you want to upgrade from a detected legacy (1.x) installation, enter `Y`. Otherwise, enter `N`.  
If you chose to upgrade, do the following:
  - a) To copy the LDAP server configuration from the legacy installation, enter `Y`. Otherwise, enter `N`.
  - b) If you chose to copy the LDAP server configuration, enter the passwords for the LDAP servers.
  - c) To uninstall the legacy installation, enter `Y`. Otherwise, enter `N`.
  - d) To create a backup file of the legacy installation configuration, enter `Y`. Otherwise, enter `N`.  
See the info messages on the command line to see where the backup file is stored.

If an HA configuration is detected, the cluster information and associated certificates are migrated.

- 5) Select **Join existing cluster** as the role of the node.

## Next steps

- 1) Continue performing the initial setup.
- 2) Perform this task again on the other cluster members.

### Related tasks

[Configure the host firewall on page 15](#)

[Install the User ID Service on page 17](#)

[Start the initial setup on page 19](#)

## Show the status of the User ID Service

Use the Configuration Utility to check the status of the User ID Service. In an HA configuration, the status of all the cluster members is shown.

### Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.
- 2) Enter the following command:

```
fuid-cfg status
```

### Result

You are shown detailed information, such as information about the services that run in the User ID Service.

If you have configured HA, you can also see the status of the cluster members. When HA is successfully configured, the value for the `is_available` and `is_live` columns is `true`.

### Related information

[Using the User ID Service and DC Agent in an HA configuration on page 85](#)

## Update the list of cluster members

If you later add additional cluster members, you must update the configuration on all cluster members.



#### Tip

In many cases, the default option is shown. To use the default option, press **Enter**.



#### Tip

Press **Ctrl+C** to cancel an action.

### Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.

- 2) Enter the following command:

```
fuid-cfg db
```

- 3) Enter the IP address of the server that the CockroachDB database is installed on.
- 4) Enter a comma-separated list of IP addresses that represent the other servers in the cluster.
- 5) When prompted to restart the associated service, enter **Y**.

## Next steps

Perform this task again on the other cluster members.

# Overview to configuring HA for the DC Agent

Complete the following high-level steps to configure HA for the DC Agent.

- 1) Install and configure the DC Agent on more than one server.
- 2) If the User ID Service is used in an HA configuration, configure backup cluster members for all DC Agent instances.

### Related tasks

[Install the DC Agent on page 73](#)

## Enable HA for the DC Agent

If HA has been configured for the User ID Service, you can define additional User ID Service cluster members to which the DC Agent can send data.

### Before you begin

Create User ID Service API user accounts for each cluster member.

## Steps

- 1) Log on to the Windows server using administrator credentials.
- 2) Browse to the `C:\Program Files\Forcepoint\DCAgent` directory.

- 3) Open the file `config.json` with a text editor such as Notepad.
- 4) In the `fuid_servers` section, add the addresses of the cluster members, separated by commas.

Example:

```
"fuid_servers": [  
  "https://10.10.10.1:5000",  
  "https://10.10.10.2:5000",  
  "https://10.10.10.3:5000"  
],
```

- 5) Save the file.
- 6) Use the Windows Services tool to restart the DC Agent service.

## Result

If the first cluster member in the list becomes unresponsive, the DC Agent starts sending user and IP address data to the next member in the list.

## Next steps

For optimal HA for the DC Agent, install and configure the DC Agent on additional servers, and add all the cluster members to the DC Agent configuration.

# Integrating Forcepoint NGFW as the User ID Service Client Product

### Contents

- Overview to configuring Forcepoint NGFW on page 93
- Configuring certificates for Forcepoint NGFW on page 93
- Create a Forcepoint User ID Service element on page 97
- Select the Forcepoint User ID Service element for the NGFW Engine on page 99
- Verifying that the SMC is receiving data from the User ID Service on page 100

To integrate the Forcepoint NGFW as the User ID Service Client Product, you must configure various settings in the Management Client component of the SMC (SMC Management Client).

## Overview to configuring Forcepoint NGFW

---

Follow these high-level steps in the SMC Management Client to integrate Forcepoint NGFW as the User ID Service Client Product.

- 1) Configure certificates to secure communications between Forcepoint NGFW and the User ID Service.
- 2) Create a Forcepoint User ID Service element.
- 3) Add the Forcepoint User ID Service element to the NGFW Engine.
- 4) Verify that the SMC is receiving data from the User ID Service.

You can optionally configure the User ID Service to forward log data to the Forcepoint NGFW.

## Configuring certificates for Forcepoint NGFW

---

In a simple setup, you can use the self-signed certificate from the User ID Service to secure communications.

In an enterprise environment with existing certificate signing services, we recommend that you use those certificates to secure communications. For more information about certificates, see the *Forcepoint Next Generation Firewall Product Guide*.

To use the self-signed certificate from the User ID Service, complete the following high-level steps.

- 1) Copy the self-signed certificate from the User ID Service server to a location accessible to the SMC Management Client.
- 2) In the SMC Management Client, import the certificate to create a Trusted Certificate Authority.
- 3) Create a TLS Cryptography Suite Set element that defines the allowed cryptographic algorithms.
- 4) Create a TLS Profile element that defines the settings for cryptography, trusted certificate authorities, and the TLS version used in TLS-protected traffic.
- 5) Create a Forcepoint User ID Service element, then add the TLS Profile to the element.

In an HA environment, we recommend that you create certificate requests from each cluster member, and sign the requests using an external CA. In the SMC Management Client, import that CA as a Trusted Certificate Authority element, then add the trusted CA to the TLS Profile element.

If you use self-signed certificates from each cluster member in an HA environment, make sure that the certificates have a unique Distinguished Name, but a TLS server identity attribute that is the same in all the certificates, such as an IP address or DNS name. In the SMC Management Client, use the certificates to create Trusted Certificate Authority elements, then add the trusted CAs to the TLS Profile element.

#### Related concepts


Using externally-signed certificates on page 52



## Create a Trusted Certificate Authority element

Import the self-signed certificate from the User ID Service to create a Trusted Certificate Authority element.

### Before you begin

Copy the `server.crt` certificate from the `/etc/fuid` directory on the User ID Service to a location accessible to the SMC Management Client.

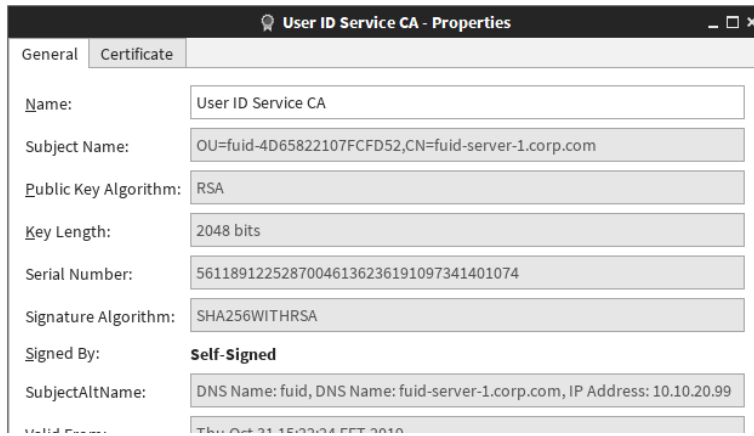
**Steps**  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select  **Configuration**, then browse to **Administration**.
- 2) Browse to **Certificates > Certificate Authorities > Trusted Certificate Authorities**.
- 3) Select  **New > Trusted Certificate Authority**
- 4) In the **Name** field, enter a unique name.  
No other fields on the **General** tab can be edited. The fields are filled in automatically based on the information contained in the certificate that you import.

- 5) On the **Certificate** tab, click **Import** to import the certificate.
  - a) Click **Import**.
  - b) Browse to the certificate, then click **Open**.
  - c) Click **OK**.
- 6) Click **OK**.

## Result

When you open the Trusted Certificate Authority element, the certificate details are shown.



## Next steps

Create a TLS Cryptography Suite Set element that contains the cryptographic algorithms that you want to use.

# Create a TLS Cryptography Suite Set element

TLS Cryptography Suite Set elements define which cryptographic algorithms are allowed for encrypting TLS traffic.

The system element NIST (SP 800-52) Compatible SSL Cryptographic Algorithms allows SSL cryptographic algorithms that are compatible with the following standard: *NIST SP 800-52 Rev. 1 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*.

If the system element meets your needs and contains the algorithms selected in the User ID Service, there is no need to create a custom TLS Cryptography Suite Set element.

**Steps** For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select **Configuration**, then browse to **Administration**.
- 2) Browse to **Certificates > Other Elements > TLS Cryptography Suite Sets**.
- 3) Select **New > TLS Cryptography Suite Set**.

- 4) In the **Name** field, enter a unique name.
- 5) Select one or more cryptographic algorithms.  
The selected algorithms must match the algorithms selected in the User ID Service.
  - Algorithms in the **Common** section are compatible with SSL 3.0, TLS 1.0, TLS 1.1, and TLS 1.2.
  - Algorithms in the **TLS 1.2 Only** section are only compatible with TLS 1.2.

The User ID Service uses the Go Language TLS module. TLS 1.3 algorithms are used first, then TLS 1.2 algorithms. For more information, see <https://golang.org/pkg/crypto/tls/>.
- 6) Click **OK**.

## Next steps

Create a TLS Profile.

# Create a TLS Profile

In the Management Client component of the SMC, create a TLS Profile element. The element defines the settings for cryptography, trusted certificate authorities, and the TLS version used in TLS-protected traffic.

**Steps** ⓘ For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select **Configuration**, then browse to **Administration**.
- 2) Browse to **Certificates > Other elements > TLS Profiles**.
- 3) Select **New > TLS Profile**.

The screenshot shows a dialog box titled "User ID Service TLS Profile - Properties". It contains the following fields and controls:

- Name:** A text input field containing "User ID Service TLS Profile".
- TLS Cryptography Suite Set:** A dropdown menu showing "User ID Service Cryptographic Algorithms" with a "Select..." button to its right.
- Trusted Certificate Authorities:** A section with two radio buttons: "Trust any" (unselected) and "Trust selected" (selected). Below the radio buttons is a list box containing "Forcepoint User ID Service CA". To the right of the list box are "Add..." and "Remove" buttons.
- Version:** A dropdown menu showing "TLS 1.1".

- 4) In the **Name** field, enter a unique name for the element.
- 5) In the **TLS Cryptography Suite Set** field, select the TLS Cryptography Suite Set element that you created. You can also select a default system TLS Cryptography Suite Set element if the allowed cryptographic algorithms are suitable.



- 6) In the **Trusted Certificate Authorities** section, select **Trust selected**.
- 7) Click **Add**, then select the Trusted Certificate Authority element that you created.
- 8) From the **Version** drop-down menu, select the minimum TLS version to use.
- 9) Configure the additional settings, then click **OK**.

## Next steps


Create a Forcepoint User ID Service element, then select the TLS Profile to use.



# Create a Forcepoint User ID Service element

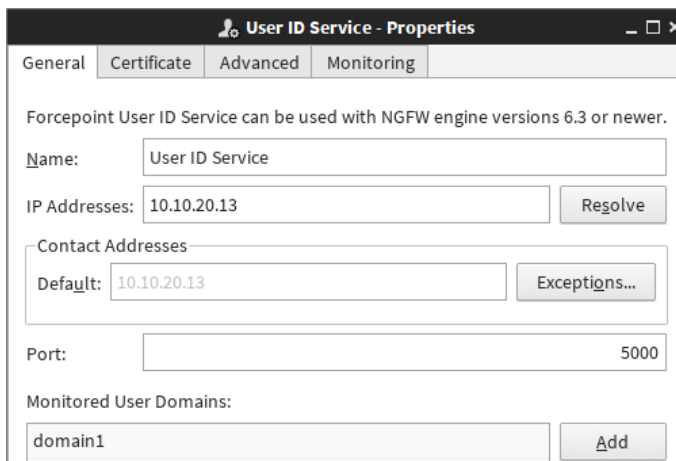
In the Management Client component of the SMC, create an element that represents the User ID Service.

## Before you begin

Create a TLS Profile.

**Steps**  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select  **Configuration**.
- 2) Browse to **Other elements > Engine Properties > User Identification Services**.
- 3) Select  **New > Forcepoint User ID Service**.

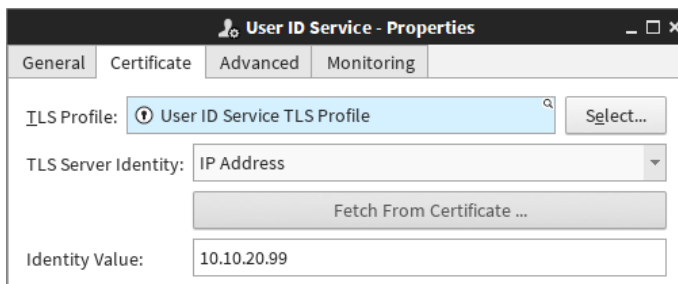


The screenshot shows the 'User ID Service - Properties' dialog box with the following fields and values:

- Name:** User ID Service
- IP Addresses:** 10.10.20.13
- Contact Addresses:** Default: 10.10.20.13
- Port:** 5000
- Monitored User Domains:** domain1

- 4) In the **Name** field, enter a unique name for the element.

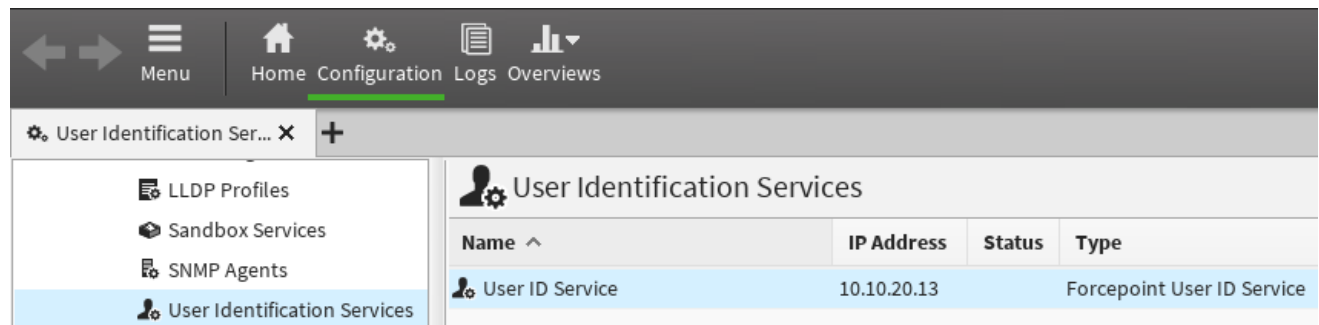
- 5) In the **IP Addresses** field, enter the IP address of the server on which the User ID Service is installed. In an HA configuration of the User ID Service, add the IP addresses of all the cluster members, separated by commas.
- 6) Enter the port that you configured the User ID Service to communicate on. The default port is 5000.
- 7) In the **Monitored User Domains** section, click **Add** to define an Active Directory domain from which the NGFW Engine receives user information.
- 8) On the **Certificates** tab, select the TLS Profile that you created for use with the User ID Service.
- 9) (Optional) From the **TLS Server Identity** drop-down list, select a TLS server identity. If you use self-signed certificates from each cluster member in an HA environment, make sure that the certificates have a unique Distinguished Name, but a TLS server identity attribute that is the same in all the certificates, such as an IP address or DNS name.
- 10) If you selected a TLS server identity, enter the value for the identity in the **Identity Value** field. If the TLS server identity is **Distinguished Name**, **SHA-1**, **SHA-256**, **SHA-512**, or **MD5**, you can click **Fetch Certificate** to fetch the value from a certificate.



- 11) (Optional) To forward log data from the User ID Service, configure the settings on the **Monitoring** tab. For more information, see the section about forwarding log data to the SMC.
- 12) Click **OK**.

## Result

The User ID Service element is created.



## Next steps

Edit the properties of the NGFW Engine, then add the Forcepoint User ID Service element to the configuration.

### Related tasks

Configure the SMC to receive log data on page 66

# Select the Forcepoint User ID Service element for the NGFW Engine

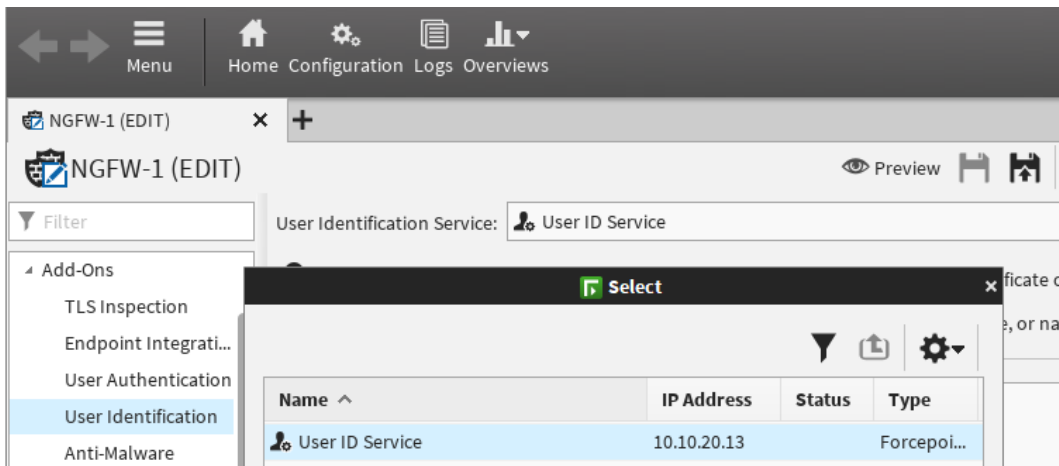
In the properties of the NGFW Engine, select the Forcepoint User ID Service element that you created.

## Before you begin

Create the Forcepoint User ID Service element.

**Steps** For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select **Configuration**.
- 2) Right-click an NGFW Engine, then select **Edit <element type>**.
- 3) Browse to **Add-Ons > User Identification**.
- 4) From the **User Identification Service** drop-down menu, click **Select**, then select the Forcepoint User ID Service element that you created.



- 5) (Optional) To prevent the NGFW Engine from receiving too many logon events, specify the IP address ranges of networks from which to receive logon events.



#### Note

Network filters do not exclude other IP addresses outside of the specified IP address range if a user has at least one logon in the specified IP address range. The NGFW Engine might still receive logon events from other IP address ranges.

- 6) Click **Save and Install**.

## Next steps

If there is a Firewall between the User ID Service server and the NGFW Engine, create an Access rule in the Firewall policy to allow communication between the User ID Service server and the NGFW Engine.

For more information about Access rules, see the *Forcepoint Next Generation Firewall Product Guide*.

# Verifying that the SMC is receiving data from the User ID Service

You can view information in the SMC Management Client to verify that the integration is working as expected. For more information about the Home and Logs views, see the *Forcepoint Next Generation Firewall Product Guide*.

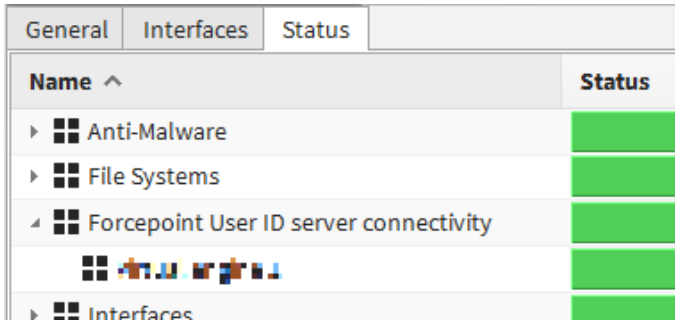
## Check the status of the NGFW Engine

You can see the NGFW Engine status in the Home view.

**Steps** For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select **Home**.
- 2) Select the NGFW Engine.  
If the NGFW Engine is a cluster, select an individual node.
- 3) In the **Info** pane, click the **Status** tab.  
If the pane is not open, select **Menu** > **View** > **Panels** > **Info**.

- 4) Verify that the status for the User ID Service connectivity is green.



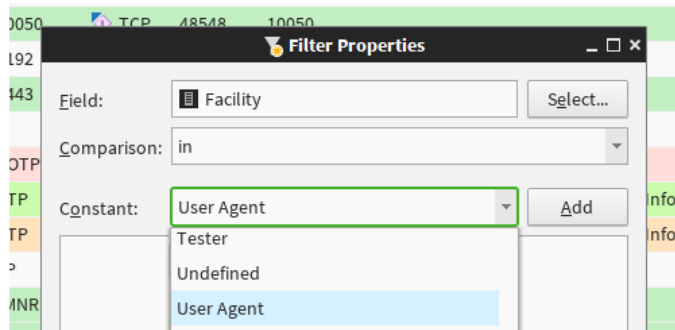
Name ^	Status
▶ Anti-Malware	Green
▶ File Systems	Green
◀ Forcepoint User ID server connectivity	Green
▶ Interfaces	Green

## Check the status in the Logs view

You can see the relevant Situations referenced in log data entries in the Logs view.

**Steps** For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select **Logs**.
- 2) Create and apply a filter.  
Use the **Facility** field and **User Agent** constant as a filter.



- 3) Verify that you see log data entries that reference the relevant Situations.  
The names of the relevant Situations begin with **FUID\_**.



### Contents

- Show the User ID Service version on page 103
- Upgrade the User ID Service and the DC Agent on page 104
- Uninstall the User ID Service and the DC Agent on page 107
- Backing up and restoring the User ID Service configuration on page 109
- Reset the User ID Service configuration on page 110
- Collect configuration and server log data for troubleshooting on page 111

Maintenance tasks include upgrading or uninstalling the User ID Service and the DC Agent.

## Show the User ID Service version

---

You can check the version information for the User ID Service.

### Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.

- 2) Enter the following command:

```
fuid-cfg --version
```

Or to get more extensive version information:

```
fuid-cfg --version-full
```

### Result

The version information is shown.

# Upgrade the User ID Service and the DC Agent

We recommend that you upgrade both the User ID Service and the DC Agent when a new version is available.

## Upgrade overview

Complete the following high-level steps to upgrade the User ID Service and DC Agent.



### Note

It is not possible to upgrade from DC Agent version 1.x. You must uninstall the previous version before installing DC Agent 2.0 or higher.

- 1) Obtain the installation files for the new versions of the User ID Service and DC Agent.
- 2) Install the new version of the User ID Service. The existing installation is detected and upgraded when you perform the initial setup.
- 3) If you use the User ID Service in an HA configuration, install the new version on the additional servers.



### Note

When you upgrade, there is system downtime even in an HA configuration.

- 4) Install the new version of the DC Agent.
- 5) If you use the DC Agent in an HA configuration, install the new version on the additional servers.

## Obtaining installation files

Download the installation files, then check the file integrity.

## Download installation files

Download the installation files from the Forcepoint website.

- The User ID Service installer is provided as a .run file.
- The DC Agent installer is provided as a .exe file.

### Steps

- 1) Go to <https://support.forcepoint.com/Downloads>.
- 2) Enter your license code or log on using an existing user account.



- 3) Click **All Downloads**, then browse to the **Network Security** section.
- 4) Under **User ID Service**, select **All versions**.
- 5) Download the installers for the version that you want to install.



#### Important

Download the same version of the User ID Service and DC Agent installers.

## Check the file integrity

Before running the installers, check that the installer files have not become corrupt or been changed. Using corrupt files might cause problems at any stage of the installation and use of the system.

### Steps

- 1) Look up the correct checksum in the [Release Notes](#) or on the Downloads page at <https://support.forcepoint.com/Downloads>.
- 2) Open a command prompt, then go to the directory where you saved the installer file.
- 3) Generate a checksum of the file, where `<filename>` is the name of the installation file.  
From a Linux command prompt, enter:

```
sha256sum <filename>
```

From a Windows PowerShell prompt, enter:

```
Get-FileHash <filename>
```

- 4) Verify that the checksum matches the checksum listed in the Release Notes or on the Downloads page.



#### CAUTION

Do not use files that have invalid checksums. If downloading the files again does not help, contact [Forcepoint Customer Hub](#).

## Upgrade the User ID Service

We recommend that you upgrade the User ID Service when a new version becomes available.



#### Note

If you use the User ID Service in an HA configuration, first upgrade the master node, then the replica nodes.

## Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.
- 2) In the directory where you saved the User ID Service `.run` installation file, enter the following command:
 

```
bash <installer-name>
```
- 3) Press **Enter** to scroll through the License Agreement, then enter `Y` to accept the agreement.
- 4) Select **Upgrade**.
- 5) When prompted to confirm your action, enter `Y`.  
The User ID Service is upgraded.
- 6) If you upgraded from User ID Service version 2.0.0 to version 2.1.0 or higher, perform either of the following actions after the upgrade is complete:
  - Restart the server on which the User ID Service is installed.
  - Enter the following commands to manually restart the UID Server and CockroachDB services:

```
systemctl restart fuid
systemctl restart cockroach
```

## Next steps

- If you use the User ID Service in an HA configuration, upgrade the User ID Service on the replica nodes.
- Upgrade the DC Agent.

# Upgrade the DC Agent

We recommend that you upgrade the DC Agent after you have upgraded the User ID Service.



### Note

It is not possible to upgrade from DC Agent version 1.x. You must uninstall the previous version before installing DC Agent 2.0 or higher.

## Steps

- 1) Log on to the Windows server using credentials that allow you to install software.
- 2) Browse to the directory where you stored the installer, then double-click the `.exe` file.
- 3) To start the installation, click **Next**.
- 4) Read the end-user license agreement, select **I accept the terms in the License Agreement**, then click **Next**.

- 5) Click **Install**.
- 6) When the installation has completed, click **Finish**.

## Result

The DC Agent is upgraded.

## Next steps

If you use the DC Agent in an HA configuration, upgrade additional installations of DC Agent.

# Uninstall the User ID Service and the DC Agent

If necessary, you can uninstall the User ID Service and the DC Agent.

## Uninstall the User ID Service

Use the User ID Service installer to uninstall the User ID Service.

You must have the installer for the currently installed version of the User ID Service. If you no longer have access to that version of the installer, you can do one of the following:

- Upgrade the User ID Service, then uninstall using the newer version of the installer.
- Manually uninstall the User ID Service.

## Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.
- 2) In the directory where you saved the User ID Service `.run` installation file, enter the following command:

```
bash <installer-name>
```

- 3) Press **Enter** to scroll through the License Agreement, then enter `Y` to accept the agreement.
- 4) Select **Uninstall**.
- 5) When prompted to confirm your action, enter `Y`.

## Result

The User ID Service is uninstalled.

## Next steps

If you use the User ID Service in an HA configuration, uninstall the User ID Service on the other cluster members.

# Manually uninstall the User ID Service

If you no longer have the installer for the currently installed version of the User ID Service, you can manually uninstall the User ID Service.

## Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.

- 2) Stop and disable the User ID Service services.  
Enter the following commands:

```
systemctl stop fuid
systemctl stop cockroach
systemctl disable fuid
systemctl disable cockroach
```

- 3) Remove the User ID Service binary components.  
Enter the following command:

```
rpm -e fuid-server cockroach
```

- 4) (Optional) Remove the User ID Service configuration folders and files.  
Enter the following commands:

```
rm -rf /etc/fuid
rm -rf /var/lib/cockroach
```

## Result

The User ID Service is uninstalled.

## Next steps

If you use the User ID Service in an HA configuration, uninstall the User ID Service on the other nodes.

# Uninstall the DC Agent

Use the Windows Control Panel to uninstall the DC Agent.

## Steps

- 1) Log on to the server with credentials that allow you to uninstall software.

- 2) Open the Windows Control Panel, then locate the DC Agent in the list of installed programs.
- 3) Right-click the DC Agent, then select **Uninstall/Change**.

## Result

The DC Agent is uninstalled. If some DC Agent files have not been removed, you can delete them manually.

## Next steps

If you use the DC Agent in an HA configuration, uninstall other installations of DC Agent.

# Backing up and restoring the User ID Service configuration

---

You can back up the User ID Service configuration to a compressed archive. You can later use the backup file to restore the configuration.

## Back up the configuration

---

Use the Configuration Utility to back up the User ID Service configuration.

### Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.
- 2) Enter the following command:

```
fuid-cfg backup
```

To manually specify a path and a file name, use the following flag:

```
-o, --out string
```

The specified path must already exist.

## Result

An archive file containing the configuration is created.

# Restore the configuration

Use the Configuration Utility to restore the User ID Service configuration.

## Before you begin

Create a configuration backup archive file.



### Note

When you restore the configuration, all data in the CockroachDB database is deleted. To repopulate the database, you must synchronize with the configured LDAP servers.

## Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.

- 2) Enter the following command:

```
fuid-cfg restore <path to backup archive>
```

If you are restoring a cluster member as part of an HA configuration, use the following flag:

```
-j, --join
```

- 3) When prompted to confirm your action, enter `Y`.

## Result

The configuration is restored.

### Related information

[Configure the LDAP server synchronization frequency on page 45](#)

[Synchronize with the LDAP server manually on page 47](#)

# Reset the User ID Service configuration

To reset the User ID Service configuration, perform the initial setup again.



### Important

Do not reset the configuration of the User ID Service to default values unless you have been instructed to do so by [Forcepoint Customer Hub](#).

## Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.
- 2) Enter the following command:

```
fuid-cfg setup
```

The existing configuration is detected, and you are prompted to remove the configuration.

- 3) When prompted to confirm your action, enter `Y`.

## Result

The entire existing configuration is removed, including the contents of the CockroachDB database and all certificates.

## Next steps

Continue performing the initial setup to configure the User ID Service again.

### Related information

[Perform initial setup of the User ID Service on page 19](#)

# Collect configuration and server log data for troubleshooting

If instructed by Forcepoint support, you can collect configuration and server log data to send for troubleshooting. No passwords or similar confidential data is collected.

## Steps

- 1) Log on to the server as root.  
You can also use `sudo` when you enter commands.
- 2) Enter the following command:

```
fuid-cfg support
```

## Result

A file named `fuid-support-<version>_<server-name>_<timestamp>.zip` is saved in the current directory.

## Using metrics

---

If you are experiencing poor performance, [Forcepoint Customer Hub](#) might ask you to enable the metrics service for troubleshooting purposes.

If you have an external Graphite server, you can configure the server with the User ID Service details to store and graph metrics data.

## Enable metrics

---

Use the Configuration Utility to enable metrics.

### Steps

1) Log on to the server as root.  
You can also use `sudo` when you enter commands.

2) Enter the following command:

```
fuid-cfg metrics enable
```

To set the frequency for metrics data to be generated, use the following flag:

```
-f, --frequency [SECONDS]
```

Where `[SECONDS]` is the frequency in seconds. The default frequency is 300 seconds.

3) When prompted to restart the associated service, enter `Y`.

### Result

Metrics are now collected.

## Show the metrics configuration

---

Use the Configuration Utility to show the current configuration.

### Steps

1) Log on to the server as root.  
You can also use `sudo` when you enter commands.

2) Enter the following command:

```
fuid-cfg metrics show
```

### Result

A summary of the current configuration is shown.



# Disable metrics

---

If you no longer need to collect metrics data, use the Configuration Utility to disable metrics.

## Steps

1) Log on to the server as root.  
You can also use `sudo` when you enter commands.

2) Enter the following command:

```
fuid-cfg metrics disable
```

3) When prompted to restart the associated service, enter `Y`.

## Result

Metrics are no longer collected.



# Appendix

## Contents

- Default communication ports for the User ID Service on page 115
- Copyrights and trademarks on page 115

## Default communication ports for the User ID Service

By default, the following ports are used in the communication between the User ID Service components.

Contacting host	Listening host	Ports
User ID Service Client Product, such as Forcepoint NGFW	User ID Service	5000/TCP
User ID Service	LDAP server	3268/TCP For LDAPS, 3269/TCP
Cluster members in HA configuration	Cluster members in HA configuration	26257/TCP
Contacting host	User ID service LDIF listening host	SyncService ports 55832/TCP
DC Agent	DC Controller, Exchange Server	135/TCP, 137/UDP, 138/UDP, 139/TCP, 445/TCP, and 49153/TCP.
DC Agent	User ID Service	5000/TCP

## Copyrights and trademarks

For information about copyrights and trademarks for the User ID Service, see the document about Legal Notices and Acknowledgments in the `/usr/share/doc/fuid` directory. For the DC Agent, see the file `thirdparty-licenses.txt` in `C:\Program Files\Forcepoint\DCAgent`.



