



FORCEPOINT

User ID Service

Release Notes

2.1.0

Revision A

Contents

- [About this release](#) on page 2
- [System requirements](#) on page 2
- [Build number and checksums](#) on page 3
- [Compatibility](#) on page 4
- [Enhancements](#) on page 4
- [Resolved issues](#) on page 5
- [Installation instructions](#) on page 5
- [Known issues](#) on page 6
- [Find product documentation](#) on page 6

About this release

This document contains important information about the current release. We strongly recommend that you read the entire document.

The Forcepoint User ID Service (User ID Service) collects data about groups, users, and associated IP addresses from Windows Active Directory (AD) Servers, Microsoft Domain Controllers, and Microsoft Exchange Servers. The User ID Service API can also be used to provide data to the User ID Service.

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.

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.

System requirements

To use this product, your system must meet these basic hardware and software requirements.

Basic hardware requirements

You can install the User ID Service and the DC Agent on standard hardware.

Component	Minimum	Recommended
Processor	2 CPU cores (recommended speed per core: 2.5 GHz)	8 CPU cores (recommended speed per core: 2.5 GHz)

Component	Minimum	Recommended
Memory	4 GB RAM	12 GB RAM
Disk space	50 GB	100 GB

A single instance of the DC Agent can monitor multiple Domain Controllers. The number of DC Agent instances needed for your environment depends on geographic network topology and the rate of incoming logon events. In large, complex environments, we recommend that you contact [Forcepoint support](#) for guidance.

Operating systems for the User ID Service

The User ID Service supports the following operating systems and versions.

- CentOS, versions 7 and 8
- Red Hat Linux Enterprise, versions 7 and 8

Operating systems for the DC Agent

The DC Agent supports the following operating systems and versions.

- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Build number and checksums

The build number of the Forcepoint User ID Service is 137. The build number of the DC Agent for the Forcepoint User ID Service is 5.

Use checksums to make sure that files downloaded correctly.

- `fuid-server-2.1.0-137.run`

```
SHA1SUM:  
95deaa997428f1b0e926ab81ff6e237d6b78cc80  
  
SHA256SUM:  
e71eabe213aa59c3c02ca8737f9ee3b6fe3d317064e9632aa907b592300fb812  
  
SHA512SUM:  
baec8409a0295539dc937e2fd73e0fc6  
7ee6722d3ee3106e5883031b76f3ce2d  
2fe50faea80edd0080db57d77c17f544  
31ca22326ceaff5fd82d23a82f4eacad
```

- UID-DCAgent-2.1.0-5.exe

```
SHA1SUM:
cb29af3e219c5631562a66065375699910331391

SHA256SUM:
2e3240cf760c3947cac6b311e0b8bc49f86d32e292c78ac5cafec48da46d7c04

SHA512SUM:
cfe1a7dc28044cf86e73b590b56da6ab
7cb3fcd8f7e14a081e31049ed46ac65c
df346e96837a477f370ff72542cd6272
59c7479517e25b3b52b22c098d37e7e4
```

Compatibility

The User ID Service and the DC Agent are compatible with the following Forcepoint NGFW components.

Component	Minimum version	Recommended version
Forcepoint NGFW Security Management Center (SMC)	6.3.0	Latest 6.7.x maintenance version or higher
Forcepoint Next Generation Firewall (Forcepoint NGFW)	6.3.0	Latest 6.7.x maintenance version or higher

Compatibility of legacy (1.x) versions

Version 2.x of the User ID Service is compatible with version 1.x of the DC Agent, but we strongly recommend that you use version 2.x of both the User ID Service and the DC Agent.

Version 2.x of the DC Agent is not compatible with version 1.x of the User ID Service.

Enhancements

This release of the product includes these enhancements.

Enhancements in Forcepoint User ID Service version 2.1.0

Enhancement	Description
Additional attributes for self-signed certificates	In addition to common name and subjectAltName, the Configuration Utility now allows you to optionally configure the following additional attributes for self-signed certificates: country, state, locality, organization, and organizational unit.
Option to import an externally generated private key and certificate pair	You can now import an externally generated private key and certificate pair to secure communications between User ID Service and external components. The certificate can be in PEM or DER format. The key must be an RSA key.

Enhancement	Description
Default TLS version and cipher suites in the TLS settings have been updated	By default, the minimum TLS version for the TLS settings is now TLS 1.2. The default list of cipher suites in the TLS settings now excludes older ciphers.
API user creation during initial setup	An API user is required for communication with the DC Agent. The initial setup of the User ID Service now includes a mandatory step to create an API user.

Resolved issues

These issues are resolved in this release of the product. For a list of issues fixed in a previous release, see the Release Notes for the specific release.

Description	Issue number
When the User ID Service synchronizes group and user definitions from AD Servers, the User ID Service might fail to handle some security identifiers (SIDs).	UID-512
When you define users to ignore in the ignore.txt file, the DC Agent only takes into account one IP address mapping for each user.	UID-513
If the /etc and /var/lib directories are on different filesystems, database installation fails.	UID-514

Installation instructions

Use these high-level steps to install the User ID Service and the DC Agent.

For more information, see the document *How to integrate Forcepoint User ID Service with other Forcepoint products* in Knowledge Base article [14100](#) or at <https://support.forcepoint.com>.

Steps

- 1) Download the installation files from <https://support.forcepoint.com/Downloads>.
Make sure that you download installation packages for the same version of the products.
- 2) Prepare your environment for the installation.
- 3) Install and configure the User ID Service.
- 4) Install and configure the DC Agent.
- 5) (Optional) Install and configure additional instances of both the User ID Service and the DC Agent, for high availability (HA).
- 6) Configure the User ID Service settings in the User ID Service Client Product, such as Forcepoint NGFW.

Upgrade instructions

We recommend that you upgrade the User ID Service and the DC Agent when a new version of the products becomes available.

To upgrade the User ID Service and the DC Agent, download and run the installers for the new version.

For more information, see the document *How to integrate Forcepoint User ID Service with other Forcepoint products* in Knowledge Base article [14100](#) or at <https://support.forcepoint.com>.

Upgrading from version 2.0.0 to version 2.1.0 or higher

After you upgrade from User ID Service version 2.0.0 to version 2.1.0 or higher, you must restart the server on which the User ID Service is installed, or manually restart the UID Server and CockroachDB services.

To manually restart the UID Server and CockroachDB services, follow these steps:

- 1) Log on to the server as root.
You can also use `sudo` when you enter commands.
- 2) To restart the UID Server service, enter the following command:

```
systemctl restart fuid
```

- 3) To restart the CockroachDB service, enter the following command:

```
systemctl restart cockroach
```

Upgrading from legacy (1.x) versions

When you upgrade from User ID Service version 1.x to version 2.x, the installer prompts you to migrate the previous installation.

To upgrade from DC Agent version 1.x, you must uninstall the DC Agent before installing the new version.

Known issues

For a list of known issues in this product release, see Knowledge Base article [17717](#).

Find product documentation

On the Forcepoint support website, you can find information about a released product, including product documentation, technical articles, and more.

You can get additional information and support for your product on the Forcepoint support website at <https://support.forcepoint.com>. There, you can access product documentation, Knowledge Base articles, downloads, cases, and contact information.

Product documentation

Every Forcepoint product has a comprehensive set of documentation.

- *How to integrate Forcepoint User ID Service with other Forcepoint products*
- *Forcepoint User ID Service API Reference Guide*

For information about the Forcepoint NGFW, see the *Forcepoint Next Generation Firewall Product Guide* and the Forcepoint Next Generation Firewall online Help.

