



Identity Director

## Release Notes

2020.0.1

## Copyright Notice

This document is provided strictly as a guide. No guarantees can be provided or expected. This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as "Ivanti") and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein. For the most current product information, please visit [www.Ivanti.com](http://www.Ivanti.com).

Copyright © 2020, Ivanti. All rights reserved.

Protected by patents, see <https://www.Ivanti.com/patents>.

---

# Contents

---

<b>About this Release</b> .....	<b>4</b>
<b>What's New</b> .....	<b>5</b>
<b>Highlighted Features</b> .....	<b>5</b>
Identity Broker: Support for multiple tenants .....	5
Rebranding: New logos applied .....	5
<b>Announcements</b> .....	<b>6</b>
Deprecation of access to Management and Web Portals over HTTP .....	6
Deprecation of 'allowInFrame' attribute (Identity Director 2020.0.1) .....	6
Deprecation of support for Oracle and IBM DB2 Datastores in a next release of Identity Director .....	6
<b>Enhancements and Improvements</b> .....	<b>7</b>
Identity Broker: Support for unattended installation .....	7
Login Page services: Displaying 'Finish' button now configurable .....	7
Portals: Hardened security .....	7
Transaction Safeguard: People attribute triggers now also taken into account .....	7
<b>Bugs Fixed</b> .....	<b>8</b>
<b>Known Issues and Limitations</b> .....	<b>9</b>
<b>Additional information</b> .....	<b>15</b>

## About this Release

This table shows the Identity Director version that introduced the Datastore revision level that applies to Ivanti Identity Director 2020.0.1

Datastore revision level	Introduced in
86	Identity Director 2020.0

- During installation, the Datastore is automatically updated if it is of a lower revision level.
- For IBM DB2 databases, the database changes require that the database is created with the "Code Set" UTF-8 instead of the default IBM-1252.

# What's New

## Highlighted Features

### **Identity Broker: Support for multiple tenants**

---

When using Identity Broker authentication, you can now assign separate Identity Providers to each of the host names configured for the Web Portal URL.

Identity Broker will only use the configured Identity Provider for users being redirected from that particular Web Portal URL.

### **Rebranding: New logos applied**

---

New Identity Director product logos have been applied.

## Announcements

### **Deprecation of access to Management and Web Portals over HTTP**

---

As of Identity Director 2020.0, you can no longer access the Management and Web Portals over HTTP.

If these portals allow access over HTTP in your environment, please read known issue "Management and Web Portals: Cannot access portals over HTTP after installing Identity Director 2020.0 or higher" on page 12 before installing Identity Director 2020.0.1.

### **Deprecation of 'allowInFrame' attribute (Identity Director 2020.0.1)**

---

Because of security concerns, the `allowInFrame` attribute in the `WebPortal.config` has been deprecated as of Identity Director 2020.0.1.

If you are using the attribute in your environment, please read [this](#) known issue before installing Identity Director 2020.0 or 2020.0.1.



Identity Director 2020.0.1 contains additional changes related to this functionality (compared to version 2020.0).

---

### **Deprecation of support for Oracle and IBM DB2 Datastores in a next release of Identity Director**

---

Due to very limited use and demand, support for Oracle and IBM DB2 Datastores will be deprecated in a next release of Identity Director.

## Enhancements and Improvements

### Identity Broker: Support for unattended installation

---

Identity Broker now also supports unattended installation. See the Identity Director Help for an overview of available Public Properties.



Identity Broker as part of the Identity Director installer is now fully supported, and no longer a Technical Preview.

---

### Login Page services: Displaying 'Finish' button now configurable

---

You can now configure if the **Finish** button should be displayed at the end of the Password Reset or Account Unlock process.

This can enhance usability in scenarios where the Identity Director Web Portal is displayed as part of a generic user portal:

The button takes you to the Web Portal login page, which may be confusing to some users.

### Portals: Hardened security

---

Security for the Management Portal and Web Portal has been hardened.

### Transaction Safeguard: People attribute triggers now also taken into account

---

The Transaction Safeguard now also applies to workflows that are triggered by auto (de)provisioning based on a change in people attributes.



For links to release notes of previous versions and more, please refer to the "Additional information" on page 15.

---

## Bugs Fixed

The following issues have been resolved in release 2020.0.1:

Problem ID	Title
73266	Identity Broker: Error message The client application is not known or is not authorized when opening the Identity Broker Management Portal <a href="#">Knowledge-base article</a>
	Management and Web Portals: Error Server Error in '/identitybroker' Application. Value cannot be null. Parameter name: InstrumentationKey when attempting to log in after upgrading to Identity Broker 2020.0
	Provisioning: Automatic (de)provisioning based on date and time may not create all expected transactions

Resolved in release 2020.0:

Problem ID	Title
72339	Delegated Administration: Selecting a service multiple times from a Service panel in the Web Portal causes the list of qualified people to be empty <a href="#">Knowledge-base article</a>

# Known Issues and Limitations

## Attributes: Attributes with names that contain special characters not processed in "Provide Information" action

---

Consider the following scenario:

1. In the Management Portal at **Entitlement Catalog**, you configured a service with service attributes that contained special characters in their name (&, <, >, etc.).
2. In the service workflow, you configured a **Provide Information** action and add the attributes to a page.

In this scenario, when you requested the service, the attributes were not processed in the **Provide Information** wizard.

This is a known issue. Ivanti recommends NOT to use special characters in the names of attributes.

## Attributes: Validation of password service attributes in "Provide Information" actions fail in rare scenarios

---

In rare scenarios, the validation of password service attributes in services fail:

Consider the following scenario:

1. In the Management Portal at **Entitlement Catalog**, you configured a service that contained a **Provide Information** workflow action.
2. In the **Provide Information** action, you added a password service attribute to a page.
3. You applied user input validation to the attribute and configured a regular expression for this purpose.
4. You added a **Jump** action to the service workflow, which jumped back to the **Provide Information** action.
5. You requested the service from the Identity Director Web Portal.
6. When prompted, you provided a password that matched the configured regular expression.
7. When the service workflow jumped back to the **Provide Information** action and you were prompted again to provide a password, you did not provide a new password, but proceeded with the workflow.

In this scenario, validation of the password service attribute failed. This issue also occurred if the workflow contained two **Provide Information** actions with the same regular expression validation for the same password service attribute.

This is a known issue. Because of security reasons, Identity Director does not pass unencrypted password values from the server to the client side for validation. As a result, the same password cannot be validated twice. Ivanti recommends not to use scenarios like these. This functionality will not be changed in future releases.

### **Audit Trail: Restoring deleted service might not be possible if service was restored before**

---

Consider the following scenario:

1. In the Management Portal at **Entitlement Catalog**, you deleted a service that could be restored.
  - Several versions of the service had been saved.
2. In the Management Portal at **Audit Trail**, you used **Restore** on one of the versions of the service, that was *not* the latest version.
3. In the Management Portal at **Entitlement Catalog**, on the restored service, you restored to the latest version of the service.

In this scenario, if you deleted the service again, restore was not available for the service in the **Audit Trail**.

This is a known issue.

### **Audit Trail: Restoring deleted service not working as expected if multiple services with identical names have been deleted**

---

Consider the following scenario:

1. In the Management Portal at **Entitlement Catalog**, you deleted multiple services with identical names, that could be restored.
2. In the Management Portal at **Audit Trail**, you used **Restore** on one of the deleted services, that was *not* the last one that was deleted (service 'x').  
A list of versions that could be restored was displayed.

In this scenario, the versions that were displayed were for the service that *was* the last one that was deleted (service 'y').

Using **Restore** on a version from the list resulted in service 'y' being restored.

This is a known issue.

## Data Connections: Error when synchronizing data source with 40,000+ users on MySQL

Consider the following scenario:

- The Datastore to which your Identity Director environment connects is hosted on a MySQL database server.
- In the Setup and Sync Tool, at **Data Model > Data Sources**, you created a new data source for a CSV file. The CSV file contains at least 40,000 users.
- At **Data Model > Data Connections**, you created a new data connection of type **People**.
- On the **Mappings** tab of the data connection, you configured the mappings for **Person Name**, **Windows user account** and **Primary e-mail address**.

In this scenario, after synchronizing the data connection, the following was shown on the Diagnostics tab of the data connection:

```
Synchronization completed (0 errors, 0 warnings).
Changes: 39999 added, 0 updated, 0 deleted.
Duration: 0 hours, 24 minutes, 20 seconds.
ERROR: The connection has been disabled.
```

In the Management Portal at **People**, all users were added, despite of the message shown that the connection was disabled.

### Cause

The actual error that MySQL gives is: MySQL Error 1153 - Got a packet bigger than 'max\_allowed\_packet' bytes.

The default GLOBAL setting for `max_allowed_packet` is 16MB. However, according to the MySQL documentation, you can change this to up to 1GB (provided the server has enough memory).

The problem is actually caused with low memory on the MySQL server and the default setting for the `net_buffer_length` GLOBAL MySQL variable, which is 16KB. The reason for this low setting is that MySQL wants to make sure that no packets are broken. Although you can change this to up to 1MB according to the MySQL documentation, this is not the default value. Per SESSION, this value is read only, you cannot change it and is 16KB.

The sync log that Identity Director generates and tries to upload in the `OR_DataLinks` table can be much larger (for example almost 1MB when synchronizing a data connection for 40,000 users).

### Solution

Change the default GLOBAL settings on the MySQL database server with the following commands:

Get GLOBAL variables values	<ul style="list-style-type: none"> <li>• SHOW GLOBAL VARIABLES LIKE 'max_allowed_packet'</li> <li>• SHOW GLOBAL VARIABLES LIKE 'net_buffer_length'</li> </ul>
Set GLOBAL variables values	<ul style="list-style-type: none"> <li>• SET GLOBAL net_buffer_length = 1048576</li> <li>• SET GLOBAL max_allowed_packet=16777216</li> </ul>

### **Data Connections: Node 'Data connections' not available in Setup and Sync Tool with read-only permissions**

---

In the Setup and Sync Tool, if your administrative role has read-only permissions to the data connections node, the node will not be available. This is a known issue.

### **Data Sources: Setup and Sync Tool crashes when configuring ODBC-based data source with MySQL ODBC Connector 5.2**

---

In the Setup and Sync Tool, when you configure an ODBC-based data source with MySQL ODBC Connector 5.2, the following error may occur in the Setup and Sync Tool:

```
'AccessViolationException' - corrupted memory
```

To solve this issue, update the driver to the latest version.

### **Management and Web Portals: Cannot access portals over HTTP after installing Identity Director 2020.0 or higher**

---

In environments that (also) allow access to the Management and/or Web Portals over HTTP, these connections will fail after installing Identity Director 2020.0 or higher.

This is by design. For enhanced security, as of Identity Director 2020.0, the Management and Web Portals can only function when accessed over HTTPS.

Reconfigure the portals in Microsoft IIS to only be accessible over HTTPS.

### **Management Portal: Error when trying to Request, Return, Assign or Unassign a service for more than 2000 people at once**

---

In the Management Portal at **People**, if more than 2000 people have been selected (for example using **Preload all** and **Select all**), using the Services actions **Request**, **Return**, **Assign** or **Unassign** will return an error and the action will not be executed.

This is a known limitation.

### **Management Portal: Identity Broker error when pressing Back button in Identity Director**

---

Consider the following scenario:

1. In the Management Portal, **Login Type** is set to **Identity Broker** (at **Setup > Administrative Roles**).
2. A user logs on to the Management Portal
3. After logon, the user clicks the **Back** button of the web browser.

In this scenario, an Identity Broker error is displayed.

This is a known issue.

### **Management Portal: Installation on domain controllers not recommended**

---

Although technically possible, due to technical implications we do not recommend installing the Management Portal on a domain controller.

### **Password Reset: Transaction remains pending when specifying long verification code**

---

In the Management Portal at **Setup > Password Reset**, if you enable verification code validation, you can specify a service that generates this code via a **Provide Verification code** action. In this action, we recommend specifying a verification code of up to a maximum of 20 characters. Because the code is encrypted, longer codes may exceed the maximum value. This will result in an error and leave the transaction in a **Pending** state.

### **Setup and Sync Tool: Run as administrator on Microsoft Windows Server 2012 Essentials**

---

When you install the Setup and Sync Tool on a device running Microsoft Windows Server 2012 Essentials, the Setup and Sync Tool needs to be started with **Run as administrator**. This prevents issues in which advanced Active Directory user properties cannot be retrieved by the Setup and Sync Tool.

### **Transaction Engine: Only one Transaction Engine supported on IBM DB2**

---

In environments in which the Datastore is hosted on an IBM DB2 database server, the use of only one Transaction Engine is supported.

### **Web Portal: Web.config file overwritten when performing repair on non-default installation location**

---

Consider the following scenario:

1. You perform a clean install of the Identity Director Web Portal on a non-default installation location.
2. You customize the `web.config` file of the Web Portal to your situation.
3. After installation, you run the same installer again and choose to perform a repair.

In this scenario, the settings that were configured in the `web.config` file are not preserved.

As a workaround for this issue, please copy the settings from the backup file of the original `web.config` file and replace them in the new one.

### **Web Portal: Display in iframe not working after installing version 2020.0 or higher**

After installing Identity Director 2020.0, if you have configured the Web Portal to be displayed in an iframe using the `allowInFrame` attribute, this may no longer work.

The security enhancements in this version will ignore the `allowInFrame` attribute.

For instructions on how to restore the display, please refer to the [Identity Director Help](#).

---



Identity Director 2020.0.1 contains additional changes related to this functionality (compared to version 2020.0).

---

### **Windows Client: Connection state of client not indicated by icon in notification area**

As of version 2020.0, the icon in the notification area does not indicate the connection state of the Windows Client.

This will be resolved in a next release.

# Additional information

## Release Notes of previous versions

[Identity Director 2019.3.1](#)

[Identity Director 2019.2.1](#)

[Identity Director 2019.1.2](#)

[Identity Director 2019.0.3](#)

[Identity Director 2018.3](#)

[Identity Director 2018.2.3](#)

[Identity Director 2018.1.1](#)

[Identity Director 10.3.200.0](#)

## Compatibility Matrix

Supported Operating Systems, Database systems, Browsers, and Ivanti Products are detailed in the [compatibility matrix](#).

## Further Help and Information

Information about installing, configuring, and using Identity Director is available from the [online Help](#)