ivanti | Identity Director

# Release Notes

2020.3.1

## 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.

Copyright © 2020, Ivanti. All rights reserved.

Protected by patents, see https://www.ivanti.com/patents.

# Contents

Copyright © 2020, Ivanti. All Rights Reserved. Privacy and Legal.

# About this Release

This table shows the Identity Director version that introduced the Datastore revision level that applies to Ivanti Identity Director 2020.3.1

| Datastore revision level | Introduced in |
|---|---|
| 90 | Identity Director 2020.3 |

- During installation, the Datastore is automatically updated if it is of a lower revision level.

Copyright © 2020, Ivanti. All Rights Reserved. Privacy and Legal.

# What's New

## Highlighted Features

### Extended Smart Rules allowing for employees to have multiple managers

There are cases when multiple managers or coordinators need to be able to trigger various entitlements for the same employees. By introducing a new People attribute of type List (see here) , Identity Director can now leverage smart rules to allow multiple people to be served by multiple coordinators through the Delegated Administration panels.

Two new Smart Rules have been updated to support the new List attribute:

- Manager of Subscriber
- Subordinates of Subscriber

### Data Connections upgrade – Two types of attributes can now be synchronized via Data Connections: Table and List (New)

The addition of a People attribute of type List (see here) in Identity Director 2020.3 has also had impact on data connections. The People Table Attributes data connection has been renamed to “People Attributes”.
You can synchronize data into tables or lists via this single data connection type. The choice between table and list can be made using a simple drop-down in the configuration.

Using the List attribute does not contain the advanced data mapping and merging capabilities of the table attributes.

### Allow people Identifiers and Attributes to be visible in Delegated Administration, on person details

In large organizations, people may share the same name. When this happens, managers and coordinators often find it hard to identify the correct person.

For that reason, people identifiers are now visible in Delegated Administration.
In addition to that, when defining a people attribute in the Management Portal at **Data Model**, you can specify if the attribute should be visible in Delegated Administration.

This allows for a more thorough diagnostic when making decisions regarding entitlement allocation from the Web Portal.

Copyright © 2020, Ivanti. All Rights Reserved. Privacy and Legal.

# Announcements

## Deprecation of support for Oracle and IBM DB2 Datastores as of Identity Director 2020.1

Due to very limited use and demand, support for Oracle and IBM DB2 Datastores has been deprecated as of Identity Director 2020.1.

Copyright © 2020, Ivanti. All Rights Reserved. Privacy and Legal.

# Enhancements and Improvements

The following enhancements and improvements have been introduced in release 2020.3.1:

## Retry Mechanism for Run Book results

The **Invoke Run Book** action is used to invoke a Run Book in an Ivanti Automation environment.

If the specified Run Book contains Run Book Parameters where the **Action** is set to **Get Final Value** or **Both**, the **Run Book Results** tab of the **Invoke Run Book** action allows you to let the value of service attributes depend on Run Book Parameters. These values are set during execution of the Run Book. After execution of the Run Book has finished, the Run Book results need to be retrieved by the Transaction Engine.

In case the first retrieval isn’t successful, the new retry-mechanism will initiate up to four additional attempts. The first retry will start 30 seconds after the initial retrieval attempt. Each of the following retry wait intervals will be increased by an additional 30 seconds.

When a retry is successful, the service attributes values are updated based on the received Run Book Parameters results.

The retry-mechanism makes the **Invoke Run Book** action more robust in situations when external factors may interfere with the retrieval of Run Book results.

## Enhanced Transaction Engine logging for Invoke Run Book action

The Transaction Engine traces for the **Invoke Run Book** action have been enhanced, allowing for better debugging capabilities.

Introduced in release 2020.3:

## New Person attribute of type List

This new attribute type comes to complete the attribute landscape and to allow the expansion of smart rules. There are also many cases when working with a single column table could get more complicated than just having a list attribute. That is why, in this release, a new attribute of type List has been added to People.

The attribute works the same as any other attribute, it supports restricted values and can be used in the **Set People Attributes and Identifiers** workflow action, as a **Placeholder**, as a **Delivery trigger**.

Copyright © 2020, Ivanti. All Rights Reserved. Privacy and Legal.

## API Enhancements

The API for the Management Portal now supports passing data from third-party tools into the **Provide Information** workflow action. This makes integration with ITSM tools much easier, because it allows for passing multiple types of information into Identity Director workflows in the form of a text attribute.

In addition, the API now has an endpoint allowing the administrator to choose in which organization to place the user when doing an addition or modification operation.

## Allow wildcards to be used in People attribute values for Qualification

Identity Director 2020.2 introduced the feature allowing the qualification of entitlements to be done using People attributes. Multiple instances could be added to assure for instance, that all roles inside an organization are covered.

In Identity Director 2020.3 an extra enhancement reduces the effort even more, by allowing the usage of wildcards. Following the given example, this allows the simple usage of “role name*”, which in turn covers a wide selection without the need for multiple specific additions.

## Create Administrative Roles with cross-domain groups

Identity Director now also supports cross-domain groups when creating **Administrative Roles**. This allows for users in different domains to be added to the same group and then to leverage that whole group in the creation of **Logins** for **Administrative Roles**.

**Administrative Roles** can be configured in the Management Portal, at **Setup > Administrative Roles**.

## Increased CAPTCHA security

The CAPTCHA implementation has been revised and strengthened. The new improved solution brings a more secure approach that:

- Does not allow reuse of the captcha
- Does not disclose account existence
- Does not disclose account lockout status

## Added diagnostic capabilities to the Password Complexity profiles

Identity Director 2020.2 greatly improved on password complexity, allowing for the creation of personalized and granular profiles. This made it possible to have many profiles inside Identity Director, fit even for the most demanding policies out there.

Identity Director 2020.3 now adds an advanced diagnostic feature, that verifies the rules that apply to any single user in the system. This way, the system administrator can check the policy implementation fast and without error.

For links to release notes of previous versions and more, please refer to the "Additional information" on page 20.

Copyright © 2020, Ivanti. All Rights Reserved. Privacy and Legal.

# Bugs Fixed

No additional issues have been resolved in release 2020.3.1.

Fixed in release 2020.3:

| Problem ID | Title |
|---|---|
| 74431 | Transaction Safeguard: Rule "One service requested for everyone in the system" triggered on a single People Attribute change<br>Knowledge-base article |
| 75245 | Disabled action freezes workflow<br>Knowledge-base article |
| 75466 | Public API: Person add fails with null reference exception<br>Knowledge-base article |
| 75574 | Service not triggered on attribute change after synchronization of Setup and Sync Tool<br>Knowledge-base article |
| 75713 | Unable to Request a service - Pending transaction -"[Service Name] could not be requested. Reason: Pending.." <br>Knowledge-base article |
| 75843 | Qualification for a service based on multiple Peoples Attributes and Organizations is not calculated correctly<br>Knowledge-base article |
| 75899 | A parameter from an Ivanti Automation Run Book is not always set in an Identity Director Service attribute<br>Knowledge-base article |

Copyright © 2020, Ivanti. All Rights Reserved. Privacy and Legal.

# 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.

Copyright © 2020, Ivanti. All Rights Reserved. Privacy and Legal.

## 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.

Copyright © 2020, Ivanti. All Rights Reserved. Privacy and Legal.

## 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 | • SHOW GLOBAL VARIABLES LIKE 'max_allowed_packet'<br>• SHOW GLOBAL VARIABLES LIKE 'net_buffer_length' |
| Set GLOBAL variables values | • SET GLOBAL net_buffer_length = 1048576<br>• SET GLOBAL max_allowed_packet=16777216 |

Copyright © 2020, Ivanti. All Rights Reserved. Privacy and Legal.

### 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.

### Entitlement qualification based on Person attributes

Consider the following scenario:

You want to add the same Person Attribute two times to include in the qualification all people related to a job role.

1. You add the people attribute called ROLE
2. You click on the Add People Attribute button next to add it again and nothing happens.

This is because to be able to add an attribute multiple times, you must add another item (either a person, a person attribute or an organization) after the attribute first and then add the necessary attribute.

Example:

1. Add the ROLE attribute
2. Add a person or an organization
3. Click on the attribute
4. Add another item
5. Add OR
6. Add the ROLE attribute

This limitation will be removed in a next release.

Copyright © 2020, Ivanti. All Rights Reserved. Privacy and Legal.

### 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.

### Management Portal: Searching entitlements based on tags not working

Although tags are defined in the Management Portal, currently you can only use them as a search argument in the Web Portal.

Copyright © 2020, Ivanti. All Rights Reserved. Privacy and Legal.

### Password History: Identity Director is not integrated at a history level with AD or other provider nor does it enforce its history on any other software system

Consider the following scenario:

1. Your Identity Director environment version 2020.1 or higher is configured to work with identities provided by both Microsoft Active Directory and Okta, through integration via the SSO component – Identity Broker.
2. User M (for 'Microsoft') is resetting the password via one of the Identity Director clients and is using Microsoft Active Directory as their identity provider.
   This user is reusing their old password.
3. User O (for 'Okta') is resetting the password via one of the Identity Director clients and is using Okta as their identity provider.
   This user is also reusing their old password.
4. The password reset process fails for user O and user M, but without any further details.

The expectations of IT here would be that the process should inform the user about the old password being reused in both cases. Because of integration and connector development complexities, Identity Director does not implement password history through integration, but holds its own history. This is a known limitation.

After installing version 2020.1 (or higher), Identity Director looks at both the password being changed through its clients and the passwords being used by users to log in. If the provided password does not match any of the stored, previously used passwords, it will be added to the history. This covers the case when a password is changed for users by IT directly from the identity provider.

Once the 2020.1 (or higher) release is rolled out, users can reuse their old password only once, by default. The second time this operation would be impossible. However, if IT wants to keep the same password for a longer time (which is highly unlikely, but exceptions do occur), they can do that by using Automation tasks to reset to the same password or simply change the policy in the identity provider.

Copyright © 2020, Ivanti. All Rights Reserved. Privacy and Legal.

### Password Reset: Make password complexity vary according to organizational context

Consider the following scenario:

1. In the Management Portal, at **Password Reset > Complexity**, you configure several profiles which contain organizations 'Engineering' and 'Management'.
2. You go to Organizations and rename 'Engineering' to 'Engineering Internal'.
3. You delete Management.
4. Coming back to **Password Reset > Complexity**, you go back and see that the changes have not propagated to this area.

If you delete or modify an organization in Identity Director, that modification does not propagate within the structures defined in the Password Complexity profiles. As such, any organizational change that is done once the Complexity Hints are in place, should be accompanied with a check over this area.

### 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.

### Security Questions: The experience is only implemented for the Web Portal, with follow-up improvements in 2020.2 or sooner for the other clients

Consider the following scenario:

1. In the Management Portal, at **Setup > Login Page Services > Password Reset > Security Questions**, you configure the number of attempts to try to answer the security questions before the account gets locked out.
   For example: you have 3 failed attempts and 3 questions
2. In the Web Portal, you answer all 3 questions incorrectly.

Currently, a workaround is in place that allows the Windows Client to check the locked status of a user, but the whole lockout experience is missing from the mobile apps, both Android and iOS.

This is a known issue and the follow-up implementation is expected to be released in Identity Director 2020.2, or sooner in an intermediary release.

Copyright © 2020, Ivanti. All Rights Reserved. Privacy and Legal.

### Security Questions: The limit to the number of times a question can be answered is not set per question but per set of questions

Consider the following scenario:

1. In the Management Portal, at **Setup** > **Login Page Services** > **Password Reset** > **Security Questions**, you configure the number of attempts to try to answer the security questions before the account gets locked out.
   For example: you have 3 failed attempts and 3 questions
2. In the Web Portal, you answer all 3 questions incorrectly.

In this scenario, when you click **Next** and try to get to the next step of the Password Reset process in the Web Portal, your account will be locked out for the configured amount of time as specified in the Management Portal. That is because the number of failed attempts counts the total number and not the number per question.

This is a known issue. Ivanti recommends that the whole set of questions be subject to the limitation so that a brute-force attack will be even less successful than being able to try X times per question.

### Security Questions: The message informing the user of how many attempts are left before the account is locked out is not configurable

Consider the following scenario:

1. In the Management Portal, at **Setup** > **Login Page Services** > **Password Reset** > **Security Questions**, you configure the number of attempts to try to answer the security questions before the account gets locked out.
   For example: you have 3 failed attempts and 3 questions
2. In the Web Portal, you answer one of the questions incorrectly (answer the other questions correctly) and click **Next**.
3. After each attempt, the user will be notified about the current status with the message “You have X attempts left to answer the security questions before account lockout.”
   This message is not configurable.

This is a known limitation, that should not result in much inconvenience in any typical scenario.

### 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.

Copyright © 2020, Ivanti. All Rights Reserved. Privacy and Legal.

### 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 DirectorWeb 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 and higher contain additional changes related to this functionality (compared to version 2020.0).

Copyright © 2020, Ivanti. All Rights Reserved. Privacy and Legal.

# Additional information

## Release Notes of previous versions

Identity Director 2020.2.0

Identity Director 2020.1.0

Identity Director 2020.0.1

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

## 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

Copyright © 2020, Ivanti. All Rights Reserved. Privacy and Legal.