ivanti | Identity Director

Release Notes

2020.1

Copyright Notice

Contents

About this Release

This table shows the Identity Director version that introduced the Datastore revision level that applies to Ivanti Identity Director 2020.1

Datastore revision level	Introduced in
87	Identity Director 2020.1

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

What's New

Highlighted Features

Protection from brute-force attacks - Limiting the number of tries to answer Security Questions

When using Security Questions to check for the identity claim of a user, it is now possible to limit the number of tries to answer those questions. You can set an overall limit of incorrect answers that applies to the whole set of questions and a limit of time in which, if a set of wrong answers are introduced, and a lockout triggered. Thus, in the event of a brute-force attack, the account will be locked out for a configurable amount of time.

Password Reset features now include a password history verification option to limit password reuse

One of the most sought-after features by IT when it comes from password reset, is the option to limit password reuse. In order to make this operation as easy to implement as possible, Identity Director now has a feature allowing for password history verification. The history itself is contained within Identity Director and does not come from integrations with various providers, such as Microsoft AD, Okta, etc.

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.

Enhancements and Improvements

Web Portal: A self-signed certificate can be used in unattended installation

The Web Portal now has support for using a self-signed certificate during the unattended installation process. Also, an example script has been added for guidance in installing the all product components, including Identity Broker.

Please note, that existing scripts for unattended installation of the Web Portal will have to be updated to include the new property `SELECT_CERTIFICATE`.
See the Identity Director Help for further details.

Remove identities marked "Ready for Deletion" after a set number of days

When offboarding users, an automatic process is necessary to delete the remaining data from the Datastore and possibly from AD via Automation. This keeps the offboarding process clean and less error-prone. Starting with Identity Director 2020.1, the identities marked as "Ready for Deletion" can be automatically erased after a certain amount of time.

This also solves the problem of using the same identifier again in case of onboarding people with the same name, as many admins usually forget about identities that were left in the Datastore.

Identity Broker: Using multiple claims simultaneously

Identity Broker can now be used by multiple providers at the same time. An upgrade in the Identity Director Management Portal allows you to configure claims from multiple providers using the semicolon (`;`) as a separator. This makes it possible for user A to login with, for example, Azure AD and for user B to login with Okta in the same environment.

Identity Broker: Consumer updates

The UI regarding the Consumers has been improved regarding the support of adding different numbers of redirect URIs and post logout URIs (with no direct pairing of redirect and logout URIs). Also, URL validation before submitting the redirect/logout URIs has been added.

Security Hardening: http response headers refactoring to allow customers to use Identity Director Web Portal in iframes

A new node has been added in the `WebPortal.config` file, under the parent application node: `overwriteHttpHeaders`. Here, you can overwrite the default values for these headers with data that best suits your needs.

You can also remove the headers completely, by adding the header names and making the corresponding values empty.

If the `overwriteHttpHeaders` node is missing, or is present but the header collection is empty, the default values will be used.

For links to release notes of previous versions and more, please refer to the "Additional information" on page 18.

Bugs Fixed

The following issues have been resolved in release 2020.1:

Problem ID	Title
72852	Management Portal: Transactions multi-delete by button not working if auto refresh is enabled Knowledge-base article
72933	Action 'Provide Information': Selecting Organizational Context from Cascading List doesn't work as expected Knowledge-base article
73286	Management and Web Portals: A potentially dangerous Request.Form value was detected from the client (Password="h5mWe(<Gga"). Knowledge-base article
73117	Password reset: Redirection URL in the Login page services > Password reset is not working Knowledge-base article
72381	Password reset: `forceDefaultLanguage` set to a custom language does not function when accessing the Password Reset page without opening the Web Portal login page Knowledge-base article
	Management Portal: Horizontal scroll bar is not visible in the Workflow tab of a service Knowledge-base article

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	• SHOW GLOBAL VARIABLES LIKE 'max_allowed_packet' • SHOW GLOBAL VARIABLES LIKE 'net_buffer_length'
Set GLOBAL variables values	• SET GLOBAL net_buffer_length = 1048576 • SET GLOBAL max_allowed_packet=16777216

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 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.

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.

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.

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).

Additional information

Release Notes of previous versions

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

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