Identity Intelligence 1.1
User Guide

April 2020

NetIQ

Legal Notice

Contents

About This Book

This *User's Guide* provides concepts, use cases, and contextual help for Identity Intelligence.

Intended Audience

This book provides information for individuals who use the Identity Intelligence software. Usually, these individuals have experience with identity governance activities, such as evaluating user permissions and ensuring that access rights get assigned according to organizational procedures. Users tend to be familiar with Micro Focus Identity Manager and Micro Focus Identity Governance.

Additional Documentation

The Identity Intelligence documentation library includes the following resources:

- *Administrator Guide for Identity Intelligence*, which provides information about deploying, configuring, and maintaining this product
- *Release Notes for Identity Intelligence*
- *System Requirements for Identity Intelligence*

For the most recent version of this guide and other Identity Intelligence documentation resources, visit the documentation for Identity Intelligence.

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the **comment on this topic** link at the bottom of each page of the online documentation, or send an email to Documentation-Feedback@microfocus.com.

For specific product issues, contact Micro Focus Customer Care at https://www.microfocus.com/support-and-services/.

1 Welcome to Identity Intelligence

Identity Intelligence provides interactive and reporting capabilities for identity governance data so you can perform the following types of activities:

- Provide data in the form of visuals and reports to support audits of identity governance processes
- Export data for analysis or reporting to management and other stakeholders, such as compliance officers and resource administrators
- Look for possible issues or breaches in identity governance processes and protocols
- Evaluate request and approval processes to determine their efficiency and adherence to enterprise standards, such as service level agreements (SLAs)

Depending on the data you want to analyze, you can create a **View** and explore the **Profiles** of users and access rights.

Using drivers and collectors, Identity Intelligence gathers data from data sources such as Micro Focus Identity Manager and Micro Focus Identity Governance, then sends the data to the Transformation Hub for processing and to Vertica for storage. The deployment of Identity Intelligence includes Transformation Hub and Vertica.

For information about deploying, configuring, and maintaining this product, see the *Administrator Guide for Identity Intelligence* on the Identity Intelligence documentation site.

Analyzing Identities and Access Rights

Identity Intelligence provides current and historical data, gathered from data sources such as Identity Manager and Identity Governance, for identities and access rights in your environment. You can explore the data either in a View or in the Profiles of specific users and access rights.

2 Understanding the Data in Views and Profiles

You can view current or historical details about identities, access rights, and the processes associated with granting, revoking, and certifying access rights. Each **View** provides a visually based method for exploring a wide range of process activity, while the **Profile** lets you drill into details of the specified user or access right.

The Views and Profiles are interconnected. For example, in a View you might review a request to add an access right to an identity. You can select that identity to get a list of access rights assigned to the user on the same date as the event that you selected in the View. From there, you can select one of the listed access rights to learn more about it. You can review the users assigned to that access right and how they received it. You can also change the **As of *date*** in the Profile to check whether that user still has the access right.

What is a View?

The **View** incorporates both a visualization, such as a scatterplot or bar chart, and a table of supporting data to help you analyze the following types of identity governance activities:

- Provisioning of access rights, such as requests to add a role.
- Process activity based on workflows from Identity Manager that are associated with the specified request activities.

  For example, employee Emma Belafonte logs in to Identity Manager where she requests access to the SAP application.
- Activities associated with the assignment or removal of an access right that occur outside of an Identity Manager workflow process.

  For example, someone assigned Emma the access right within the SAP application or in Active Directory.
- Activities related to access reviews that occur in Identity Governance.

Each View can provide a unique set of data, depending on its configuration. You not only specify the **type of activities** you want to see but also specify the **time frame** when the activities occurred. To include View content in presentations or reports, you can export the data as a PDF or a CSV file. However, the exported file will not include the visualization.

The **example** for using a View explores how a resource or application owner might resolve problems with the process for granting access to the resource or application.

Example for Using a View

Avanti Rana, who owns the SalesForce application, has received complaints from sales managers that requests for access take weeks to fulfill and require multiple calls for action. She knows that the workflow for granting access to SalesForce roles requires a quorum of three out of four approvers. The approval list includes the employee's manager, Yuen Lin-wei in Risk Management, Arden Herman in Sales Management, and Avanti as the resource owner. Her company has been using this process for about 12 months. Normally, Avanti prefers to wait for two of the others to approve the request before she responds, thus giving more control to the managers who know which users should have access to SalesForce.

To identify the root of the problem, Avanti creates a View that contains all requests for SalesForce that occurred in the last six months. In the scatterplot, she observes several data points that represent incomplete requests with no activity in the last week or more. As she selects each of the incomplete data points, she realizes that these requests are awaiting approval by either Arden or Yuen. Next, Avanti looks at the data points for requests that already have been approved. In the details for these activities, she sees that Yuen and Arden took as long as two weeks to respond to the requests. She wonders whether one or both of them changed positions in the company or left the company. To verify their current status, she selects Arden's name in the Summary details so she can see Arden's User Profile. Then she does the same for Yuen. Neither has changed their job status; thus, at least one of them should be reviewing and approving the access requests in a more timely manner.

She exports the data to a CSV file so she can share these results with her management and the two approvers. She also creates a screen shot of the scatterplot to show the number of pending requests that await a response from Yuen or Arden. With this data in hand, she can formulate a plan for addressing the complaints about the approval process.

What is a User Profile?

The **User Profile** provides in-depth information about a selected user for the specified time frame:

- Organization-based information, such as title and manager
- Contact information
- Accounts assigned to the user
- Access rights assigned to the user

The **example** for exploring a User Profile describes how a security analyst might investigate identities that received unauthorized access to a resource or application.

Example for Exploring a User Profile

As a systems security analyst, Mandy Rabani is investigating a breach in the Home Grown Financial application that occurred recently. The only account that accessed the application at the time was `esutton@extremelyfocused.com`.

In **Users & Entities** > **Search** > **Users**, Mandy sets the date to when they suspect that the breach occurred, then she searches for `esutton@extremelyfocused.com`. Identity Intelligence responds that no data exists for the value. In case the account had been created for the breach and deleted immediately afterward, Mandy adjusts the search date backward and checks again. She is surprised to see that the search returns one user associated with the account: Hedda Keller, who is an IT systems administrator. Mandy had suspected that the account might be associated with Elliott Sutton, also an IT systems administrator.

Mandy opens each of their profiles to check whether either of them has an access right for Home Grown Financial on the specified date. Then Mandy changes the date to **As of Now** to determine whether the accounts are still active. She makes the following notes:

	On the Specified Date	As of Now
Elliot's profile	`ejsutton@extremelyfocused.com`	`ejsutton@extremelyfocused.com`
Hedda's profile	`esutton@extremelyfocused.com`	no account listed

Mandy decides to create a View to determine when and how Elliott and Hedda got access to Home Grown Financial, as well as when Hedda's access was revoked.

For this setting...	Mandy selects...
During this time	Last 1 year
I want to know about	◆ Provisioning of access rights ◆ Approvals of access right requests
Include activities where	◆ 'Destination user' equals Hedda Keller, Elliott Sutton ◆ 'Access right' equals HGF_user
Summarize data	Activity lifecycles plotted over time

In the View, she discovers that Elliott received access a few months ago by requesting the right in Identity Manager. In Mandy's opinion, Elliott's request was approved through proper procedures. She selects the other data points in the View. One indicates a non-process instance where Hedda received the access right a day before the suspected breach. A data point just two days later indicates that Hedda's access right was removed, also through a non-process action. Mandy knows that non-process activities can occur in the original application or in Active Directory. In either case, both are outside the proper procedure for granting and removing user access to Home Grown Financial.

Mandy exports the data from the View and the two user profiles to share with her manager and Incident Command.

What is an Access Rights Profile?

The **Access Rights Profile** provides in-depth information about a selected access right for the specified time frame, such as:

- Users or accounts that have been granted the access right
- Method whereby those users or accounts obtained the access right (directly or inherited from another access right)
- Additional access rights that the user inherits when granted the specified access right
- Number of users who have inherited access rights, either granted directly or inherited through this right

The **example** for exploring an Access Rights Profile describes how a compliance officer might discover a problem where inherited access rights are granted inappropriately to an identity.

Example for Exploring an Access Rights Profile

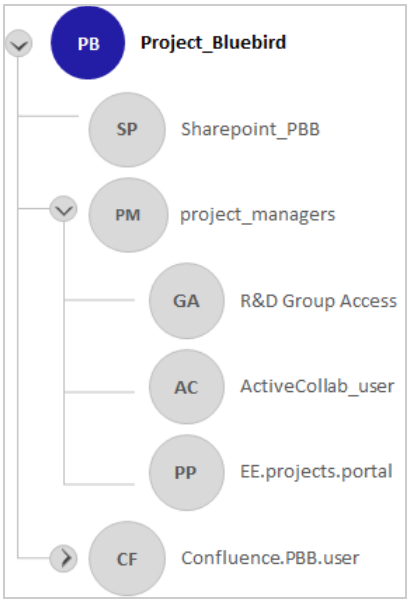
Ken in Compliance received a request from the manager of Facilities Security to investigate how an unauthorized employee was able to access a secured campus location. First, Ken calls the employee's manager, Sarah Gibson, to find out what happened. Sarah tells him that a product manager had asked her to attend a meeting with him at the R&D building, but she sent Emma Belafonte as her designate. Emma and the product manager walked over together. Since Emma was the first to the door, she naturally used her badge to enter. As a new employee, she didn't know that her badge should not have worked. The product manager expressed surprise that she had access, so Emma asked Sarah about it. Sarah, also surprised, contacted Facilities Security to report that something might be wrong with the access rights associated with Emma's badge.

Ken knows that employee badges are mapped to roles associated with specific access rights. The access right to the R&D building is `R&D_building`. Usually, employees receive that right through the `R&D Group Access` role.

In **Users & Entities** > **Search**, Ken searches for Emma Belafonte. He opens her profile to check the access rights assigned to her. She has the usual rights for a Customer Relations Specialist. However, she also has an access right called `Project_Bluebird`. Ken does not recognize `Project_Bluebird`, so he selects it. In the Access Rights Profile, he learns that Project Bluebird is a special project for the Executive Committee related to a new streaming media effort. A quick call to Sarah confirms that Emma is indeed on that project team, so the access right is appropriate for Emma.

The Access Rights Profile lists all users who have this right. Ken recognizes the names of many of the listed users. He realizes that these individuals likely have access to the R&D building, such as a vice president and an engineering director. He begins to suspect that the `Project_Bluebird` right might inadvertently grant Emma access to the R&D building. To see what access rights are also granted with `Project_Bluebird`, Ken selects **Hierarchy**. As shown in Figure 2-1, the Hierarchy chart includes access rights such as `Confluence.PBB.user`, `Sharepoint_PBB`, and `project_managers`. He expands each of the child rights to find out what rights they grant. Ken discovers that the `project_managers` access right also grants the `R&D Group Access` role. And this is how Emma was able to access the R&D building.

Figure 2-1 *Hierarchy of the Project_Bluebird Access Right*



Ken creates a report of his findings. He includes a copy of the expanded Hierarchy chart so Facilities Security can quickly see how Emma unexpectedly received the access right. He also provides recommendations for how the structure of either the `Project_Bluebird` or `project_managers` access right might be changed to mitigate future unauthorized access. As a final step, Ken sends an email to Emma and Sarah to give them a high-level view of what is happening and to expect that Emma's access to the R&D building likely will be removed.

What Kind of Data Will I Get?

Identity Intelligence gathers audit data from data sources such as Identity Manager and Identity Governance. Identity Intelligence stores the data according to its fundamental type:

Activity data

Represents user activities logged by data sources. For example, requests for roles and the approval activities associated with those requests. Or activities associated with an access review in Identity Governance. Activity data can be associated with process instances or non-process instances.

Identity Intelligence places this data in an *event datastore*.

Entity data

Represents the contextual data associated with the activities. For example, the identity, account, or group that requested the role; the name and description of the role or access right; and the identity's name and phone number.

Identity Intelligence places this data in an *entity datastore*.

In general, Views generate data from the event datastore, while Profiles access the entity datastore. However, the Views and Profiles are interconnected. When you select the name of an access right or user in a View, Identity Intelligence contacts the entity datastore to build the Profile for the selected object.

Displaying Data in a View

To reduce the amount of data points displayed in a View, Identity Intelligence consolidates all events associated with a unique request activity into a single data point referred to as a process instance. Depending on the View's criteria, these process instances might be approved, denied, or still in progress. Other data points in the View might represent non-process instances.

- "Process Instances" on page 15
- "Non-Process Instances" on page 16
- "Incomplete Data" on page 17

Process Instances

Identity Intelligence classifies most activity data as process instances. A typical **process instance** contains all events included in a single workflow process that has a common `correlation ID`, which is assigned in the data source such as Identity Manager or Identity Governance. However, some process instances represent automated workflows that don't require approval to add or revoke a request. Within the process instance, you might find the following event data:

Initiating event

Represents events such as a request for an access right.

For example, when Emma requests the HGF_user role in Identity Manager, the data contains a **Category Behavior** attribute that equals `Authorization/*/Request/Create`.

Account or user that requested the access right

Represents the user or account that either receives the access right or makes the request on behalf of someone else. For example, Sarah Gibson requests the HGF_user role for her employee Emma. In this case, the **Source Username** attribute represents Sarah while **Destination Username** represents Emma. If Emma had made the request for herself, both attributes would indicate Emma.

Access right being requested

Represents the specific access right.

For example, when Emma requests the HGF_user role, the **File Name** attribute equals `cn=HGF_user`.

System events

Represents the workflow events that the data source (such as Identity Manager or Identity Governance) creates to manage the process.

For example, assigning the task to the first approver, then forwarding the request to the next approver in the process.

Ending event

Represents the final event in the workflow process, such as a cancellation, approval, or denial of the request.

For example, the **Category Outcome** attribute equals `Success` (approved) or `Failed` (denied).

Non-Process Instances

Identity Intelligence displays non-process events only when you configure the View to summarize the events by **Activity lifecycles plotted over time**

Sometimes, individuals grant and revoke access rights without using the request process in the Identity Intelligence data sources. For example, a system administrator creates an identity for Emma Belafonte in Active Directory. Then Avanti Rana, as the resource owner of the Home Grown Financial (HGF) application, logs in to HGF to manually grant Emma Belafonte the `HGF_user` role. A few days later, Identity Manager collects the updates from HGF and Active Directory. Then Identity Intelligence collects data from Identity Manager. Upon receiving data about Emma and her access rights, Identity Intelligence stores the data in the event datastore. However, because the events occurred outside of an Identity Manager process, Identity Intelligence classifies the events as non-process instances.

In general, **non-process instances** represent actions passed from an identity data source to Identity Manager or Identity Governance. However, non-process activities might also take place within Identity Manager or Identity Governance. For example, Avanti Rana creates the `HGF_user` role in Identity Manager, and then assigns the role to Emma Belafonte. With this assignment, Avanti has bypassed the request process for that access right and identity. Other non-process instances can include the initial collection of identities and access rights from a data source. That is, the provisioning activities occurred manually in the original application or Active Directory.

Non-process instances appear in the data as standalone events because have no recognizable associations with activities that usually occur in a process instance. From the Identity Intelligence perspective, these standalone events belong in a View because they meet one of the following criteria:

- Creation, deletion, or modification of an identity
- Association of an access right with an identity or account

In the visualization of a View, Identity Intelligence indicates non-process instances with .

Incomplete Data

A data point that the View shows as **Incomplete data** represents an activity process with either a start date or end date that falls outside the specified time range.

For example, Emma requests access to the `HGF_user` role on May 29, which gets provisioned on June 3. You configure the View to display request activity from June 1 to August 31. Although Emma's request was fulfilled after June 1 (within the specified time range), the visualization shows the process as incomplete because the initial request action occurred before your time range.

If the View includes many incomplete processes at either end of the time range, you might want to modify the View criteria.

3 Analyzing Data in a View

Select **Identity Intelligence** > ***[View_name]***.

The content in a View depends on the time range and additional criteria that you specify. To build the View, Identity Intelligence pulls the results from the event datastore.

As you analyze the data, you can:

- “Explore the Visualization” on page 19
- “Manage Data in the Table” on page 20
- “Export the Table” on page 24
- “Change the View Configuration” on page 24

Explore the Visualization

The visualization contains one or more graphs to help you gain insights in the data that you requested. For example, in the visualization, you can perform the following actions:

- “View Data by Activity Status or Type” on page 19
- “Narrow the Scope of Displayed Data” on page 20
- “View Information about a Data Point” on page 20
- “Reset Views to Default Settings” on page 20

The visualization includes a legend to help you identify the categorization of the data points, such as completed processes versus incomplete ones.

View Data by Activity Status or Type

You can change the visualization to display data by the activity type or status:

Activity Status

Displays data points according to the status of their activity process. For example, *Completed* or *Denied* data processes. Or, processes with incomplete data.

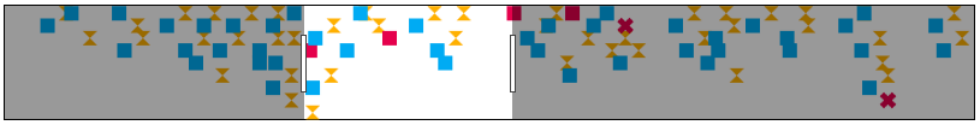
Activity Type

Displays data points according to the type of activity. For example, requests to *Add* or *Delete* an access right.

Narrow the Scope of Displayed Data

When Identity Intelligence first displays the View, the visualization includes all data points for the specified time range. If you have a large number of data points or a wide time range, you can see the big, overall picture, but you might not be able to clearly identify specific data points. To narrow the scope of the displayed data, use the mini-map that resides between the graphic and the legend.

The **mini-map** represents the entire set of queried data over the configured time range. If you adjust the outer boundaries of the mini-map, the graph and the table change to display only the data within the narrowed scope. You can also drag the narrowed section in the mini-map to the left or right.



View Information about a Data Point

You can select a data point in the visualization to review a summary of activity, such as the name of the access right that was requested, who has approved the request, and the status of the request. If you select a data point, the table updates to display only the selected data.

NOTE: If the process instance is incomplete, the details for the data point might not include the request date or the most recent approvals activity.

Reset Views to Default Settings

When you change a visualization and reopen the View, you can reset the View to its previous settings.

To reset a View to its default criteria, select the View, then click ... > **Reset to Default**.

Manage Data in the Table

You can add or remove columns in the table, as well as search for and sort data in a column. When you change the table, such as searching for a specific user, the visualization updates to match the table.

Some values must be included in the table to reduce the potential for loss of data in the visualization. For example, Identity Intelligence groups process instances by their starting event, which is represented by the value */Authorization/*/Request/Create* in the **Category Behavior** column. If you filter **Category Behavior** by the term *approval*, you remove values that include the initial request action. Thus, Identity Intelligence cannot display process instances. In a similar way, if you filter **Category Behavior** by the term *create*, Identity Intelligence sees only the starting events for the process instances. Thus, the visualization will show those processes as incomplete because you filtered out the ending events.

- "Default Attributes in the Table" on page 21
- "Attributes You Might Add to the Table" on page 22

Default Attributes in the Table

By default, the Table includes the following data attributes for most View configurations. Note that some fields might apply only to data received from Identity Governance, such as a review name.

Attribute	Description
Category Behavior	Indicates the type of action that the identity or workflow initiated For example, a */Authorization/Add/Request/Create* value indicates that someone requested a new access right or identity
Category Object	Indicates the type of object central to the action taken in the workflow process For example: ◆ *'Actor/User'* indicates that the activity might involve creating, modifying, or deleting an identity ◆ *'Host/Application/Workflow'* indicates a workflow-related action such as an identity approving a request
Category Outcome	Indicates whether the activity results in one of the following outcomes: ◆ *Attempt* represents actions that do not denote a successful or failed outcome ◆ *Success* represents an approved request ◆ *Failure* represents a request that failed to be approved
Destination Identity Given Name	Represents the given name of the identity affected by the activity
Destination Identity Family Name	Represents the family name of the identity affected by the activity
Destination Username	Represents the username, as supplied by the data source, of the identity affected by the activity For example, Identity Manager provides the username as a distinguished name (DN) Also see **Source Username** and **Destination Identity Given Name**
Device Custom String 5	*Applies only when the value for* **Device Custom String 5 Label** *equals* `correlationid` Serves as the correlation ID that groups all the activities associated with a single workflow process For example, one process instance might include the initial request action, three approval actions, and the successful closure action of the request Also see **Device Custom String 5 Label** in "Attributes You Might Add to the Table" on page 22
Device Receipt Time	Indicates when the activity occurred

Attribute	Description
File Name	Represents the name, as supplied by the data source, of the access right affected by the activity For example, Identity Manager provides DNs for the names of access rights Also see **Permission Name**
Name	Represents a short description of the activity as provided by the data source For example, *Role Request* or *Workflow Denied*
Permission Name	Represents the name of the access right affected by the activity Also see **File Name**
Source Identity Given Name	Represents the given name of the identity that generated the activity
Source Identity Family Name	Represents the family name of the identity that generated the activity
Source Username	Represents the username, as supplied by the data source, of the identity that generated the activity Also see **Destination Username** and **Source Identity Given Name**

Attributes You Might Add to the Table

To aid your investigation or understanding of identity governance activities, you might want to add some of the following attributes to the Table:

Field Name	Description
Destination Account Authority	Represents the driver that provided the data for the account that is associated with the recipient of the activity
Destination Account Name	Represents the name of the account that is associated with the recipient of the activity, as provided by the data source
Destination Account Status	Indicates whether the account that is associated with the recipient of the activity is *Active* or *Inactive*
Destination Address	Lists the address of the recipient of the activity
Destination Persona Id	Lists the identification code for the recipient of the activity For example, some companies assign an alpha-numeric ID to individuals in the organization
Destination Persona Organization	Represents the name of the department or organization to which the recipient of the activity belongs For example, *Human Resources*
Destination Persona Title	Provides the organization title of the recipient of the activity For example, *Senior Vice President*

Field Name	Description
Destination Persona Type	Indicates the category of employment or interaction with the organization for the recipient of the activity For example, *full-time* or *contractor*, depending on your organization's method for identifying an individual's status
Destination Identity Email	Provides the email address of the recipient of the activity
Destination Identity Location	Represents the location, as defined by the data source, of the recipient of the activity
Destination Identity Middle Name	Represents the middle name, if any, of the recipient of the activity
Destination Identity Phone Home	Lists the home phone number associated with the recipient of the activity
Destination Identity Phone Mobile	Lists the mobile phone number associated with the recipient of the activity
Destination Identity Phone Office	Lists the office phone number associated with the identity that initiated the activity
Device Custom String 5 Label	Represents the description of the value that the data source provides for the **Device Custom String 5** attribute In general, Identity Intelligence considers **Device Custom String 5** only when this attribute contains a value of *correlationid*
Device Product	Indicates the source of the data For example, *Identity Governance*
File Type	Indicates whether the activity relates to a **Role** or **Resource**
Message	Indicates whether the associated identity **Requested** or **Initiated** the activity
Permission Description	Provides a description of the access right based on the user-created description received from Identity Manager or Identity Governance
Source Account Authority	Represents the driver that provided the data for the account that is associated with the recipient of the activity
Source Account Name	Represents the *cn* of the account that is associated with the recipient of the activity
Source Account Status	Indicates whether the account that is associated with the identity that initiated the activity is *Active* or *Inactive*
Source Persona Id	Lists the identification code for the identity that initiated the activity For example, some companies assign an alpha-numeric ID to individuals in the organization
Source Persona Organization	Represents the name of the department or organization to which the identity that initiated the activity belongs For example, *Human Resources*
Source Persona Status	Indicates whether the identity that initiated the activity is *Active* or *Inactive*, depending on your organization's method for identifying an individual's status

Field Name	Description
Source Persona Title	Provides the organization title of the identity that initiated the activity For example, *Senior Vice President*
Source Persona Type	Indicates the category of employment or interaction with the organization for the identity that initiated the activity For example, *full-time* or *contractor*, depending on your organization's method for identifying an individual's status
Source Identity Email	Provides the email address of the identity that initiated the activity
Source Identity Location	Represents the location, as defined by the data source, of the identity that initiated the activity
Source Identity Middle Name	Represents the middle name, if any, of the identity that initiated the activity
Source Identity Phone Home	Lists the home phone number associated with the identity that initiated the activity
Source Identity Phone Mobile	Lists the mobile phone number associated with the identity that initiated the activity
Source Identity Phone Office	Lists the office phone number associated with the identity that initiated the activity

Export the Table

You can export the table to a PDF or a CSV file. To export all data, ensure that you clear all the filters. You can export only 5000 rows and 15 columns to a PDF file. To export all columns and rows, export the table to a CSV file. The exported PDF or CSV file does not contain the visualization.

Change the View Configuration

You can modify and save the settings for the View.

4 Exploring Access Right Profiles

Select **Users & Entities**.

You can view current or historical details about an access right by viewing the Access Rights Profile. For example, you might want to know which access rights were available on 29 May, and then which users had one of those rights. Identity Intelligence pulls the results from a datastore that contains historical content from data sources. Identity Intelligence uses your browser settings, such as local time zone, to display time values.

Search for an Access Right

Select **Users & Entities** > **Access Rights** > **Search**.

When you search for an access right, you can specify the point in time in which to search for and view access right information. For example, set the **As Of** date to **30 days ago** or specify a custom date and time. If you select an access right from the search results, the Access Rights Profile automatically provides information about the right according to the specified date.

Identity Intelligence uses your browser settings, such as local time zone, to display time values.

Who Has This Access Right

Select **Search Entities** > **Access Rights** > **[*Access_Right_Name*]** > **Users**.

The Access Rights Profile lists all users or accounts who have the access right in the specified point in time. For each user in the list, the profile provides the following information:

Detected on

Represents the date when the data source (such as Identity Manager or Identity Governance) indicates that the user received the access right.

For example, Avanti Rana manually assigned the HGF_user role to Emma Belafonte in the Home Grown Financial application on May 18. Then Identity Manager collected that information on May 29. The **Detected On** date equals **May 29**.

Received from

Indicates whether the user received the access right by direct assignment or inherited the right from a parent access right.

Because the data in an Access Rights Profile might change over time, you can adjust the point in time to determine which accounts or users have the access right on the specified date.

Rights Granted by an Access Right

Select **Search Entities** > **Access Rights** > **[*Access_Right_Name*]** > **Inherited Access Rights**.

The **Inherited Access Rights** tab lists all access rights that a user inherits when assigned this access right. For each of these child rights, the profile provides the following information:

- Description of the right
- Total number of users who have the right
- Number of users who received the right by direct assignment and by inheriting the right

Because the data in an Access Rights Profile might change over time, you can adjust the point in time to identify the state of the inherited rights on the specified date.

Hierarchy of an Access Right

Select **Search Entities** > **Access Rights** > **[*Access_Right_Name*]** > **Hierarchy**.

The **Hierarchy** tab provides a visual representation of both the access right and the rights that a user inherits upon receiving this access right.

Because the data in an Access Rights Profile might change over time, you can adjust the point in time to identify the hierarchy of the access rights on the specified date.

5 Exploring User Profiles

Select **Users & Entities**.

You can view current or historical details by viewing the User Profile. For example, you might want to know all the access rights that a particular user has as of 29 May of this year. Identity Intelligence pulls the results from a datastore that contains historical content from data sources such as Identity Manager and Identity Governance. Identity Intelligence uses your browser settings, such as local time zone, to display time values.

Search for a User

Select **Users & Entities** > **Search**.

When you search for a user or account, you can specify the point in time in which to search for and view user information. For example, systems analyst Mandy Rabani needs to contact the owner of the account `ejsutton@extremelyfocused.com`. So she sets the time to **As of Now**. The results indicate the account belongs to Elliot Sutton.

Identity Intelligence uses your browser settings, such as local time zone, to display time values.

In some scenarios, an identity data source may not provide a status for the identity. In such cases, the User Profile will list *Insufficient Data* for the identity in the **Status** column. For example, if Identity Governance has only minimum data required for an identity, namely *Family Name* and *CN* attributes, it will not be able to provide a status for the identity.

View Details about a User

Select **Search Entities** > **Users** > *[User_Name]* > **Details**.

The User Profile includes contact and organization information for the profile, when that data is available from the data source. For example, when search results for `ejsutton@extremelyfocused.com` list Elliott Sutton, systems analyst Mandy Rabani selects his name so she can contact him about an issue with his account. She also sees the following types of information:

- Phone number and email
- Job title
- Department
- Manager or supervisor
- Other access rights assigned to him

Because the data in a User Profile changes over time, you can adjust the point in time to observe the access rights and accounts assigned to the user.

Managing and Configuring Views

You can create, modify, and delete Views as needed.

6 Managing Your Views

Select **Identity Intelligence**.

When you create and save a View, Identity Intelligence adds the view to **My Views**. Only you can see your Views. You can add an unlimited number of Views to your list. You can also delete Views as needed.

Create

Select the View, then click +.

You can create a View at any time, based on the criteria that you specify.

Clone

Select the View, then click ... > **Clone**.

You can create a copy of an existing View by cloning it. Then you can modify the name or settings of the original or cloned View as needed.

Rename

Select the View, then click ... > **Rename**.

You can change the name or description of an existing View.

Edit

Select the View, then click ... > **Edit**.

You can change the criteria of an existing View. When you modify a View's configuration, the View returns to the default configuration. That is, Identity Intelligence removes all filters, sorts, and changes in scope that you previously made in the visualization or table.

Delete

Select one or more Views, then click ... > **Delete**.

You can delete Views one at a time or as a batch.

7 Understanding View Criteria

You can base the View on a combination of the following options:

Time Range

You can specify the start and end dates for the data that you want to view. If you select a preset time, such as **Today**, the View displays data from 12:01 a.m. to the time of day that you saved the configuration. For example, Today might be from 12:01 a.m. to 3:34 p.m. on May 29. Identity Intelligence uses your browser settings, such as local time zone, to display time values.

If one or more events in a process instance occur outside the specified time range, the View displays that instance as having incomplete data.

Type of Data to View

The **I want to know about** option allows you to specify the types of information to display in the View:

User lifecycle activities

Includes any instance related to creating, modifying, and deleting an identity. This option enables you to observe activity such as employee on-boarding and exiting.

Review of access rights

Includes any specified access rights that have been reviewed in Identity Governance. The review data indicates whether the access right should be kept or removed from the identity.

You might combine this option with **Rights assigned or removed** to not only observe the access review process but also check the processes for removing a reviewed right.

Requests to add or delete rights

Includes any instance that contains a request to add or delete the specified access rights.

For example, in Identity Manager, Emma Belafonte requests the `HGF_user` access right.

Rights assigned or removed

Includes any instance where the specified access rights are assigned or removed.

For example, a system administrator might give Emma Belafonte the `HGF_user` access right through Active Directory without Emma’s having to request the right in Identity Manager.

Approvals of access right requests

Includes workflow process instances where the specified access rights are approved or denied.

System events associated with access right requests

Includes all system activities generated by data source, such as assigning the approval task to a user that is associated with the workflow process instances.

Include and Exclude Content

You can specify the users and access rights that you want to include and exclude in the View.

For example, application owner Avanti Rana wants to see all requests to add or delete the `HGF_user` access right in the last 12 months. Except she already knows about requests made by members of her team. She makes the following selections:

For the attribute...	Avanti selects...	Avanti specifies...
Include activities where	'Access right' equals	HGF_user
Exclude activities where	'Destination user' equals	Fatima Gregory; Illiana Buckner; Hedley Velasquez

Summarize Results in a Visualization

The **Summarize data** option specifies how you want to visualize the data:

Activity lifecycles plotted over time

Creates a scatterplot that displays activities as they occurred over time.

Relative duration of activity processes

Displays a bar chart where each bar represents the time lapsed from the first event in the activity process to the last. Each process appears on the x-axis based on the most recent event.

Don't summarize data

When you choose this option, Identity Intelligence does not include a visualization in the View.

III Managing and Configuring Identity Intelligence

The product administrator must add users to Identity Intelligence, then assign them permissions according to the type of tasks that the user expects to perform.

For more information, see the *Administrator Guide for Identity Intelligence*.

8 Managing Permissions for Identity Intelligence

The **Identity Intelligence** and **Users & Entities** features require separate permission assignments.

As a user

If you have access to one feature but not the other, you might want to speak to the Identity Intelligence administrator about the permissions assigned to you.

As an administrator

Select **Admin**.

You can either assign permissions while creating users in Identity Intelligence or modify the permissions already assigned to users and roles.

You can assign specific permissions to the users. For example, if a user needs to access the entity details, you need to assign the **Access Users and Entities** permission.

For more information about assigning permissions, see the *Administrator Guide for Identity Intelligence*.

9 Renewing License

Ensure that you renew the license before its validity expires to prevent any interruption in the functionality.

To renew the license:

1. Log in to the CDF Management Portal:

   `https://<ip address or hostname of the CDF>/autopass`

2. Click **Install Licenses** > **Choose File**, browse to the location of your valid license file, and then click **Next**.
3. Click **Install Licenses** and follow the prompts to apply the license.
4. Under **View Licenses**, verify whether the license has been applied.