EVIDEN

Identity and Access Management

DirX Identity

User Interfaces Guide

Version 8.10.10, Edition June 2025

Table of Contents

Preface

This manual describes the user interfaces provided with DirX Identity for Connectivity and Provisioning. It consists of the following sections:

- Chapter 1 describes how to use the **Web Center**. The **Web Center** is a set of applications that supplies identity management functions for web usage.
- Chapter 2 describes how to use the **Web Center for Password Management**. **Web Center for Password Management** is a set of applications that supplies password management functions for web usage, and is a subset of **Web Center** functionality.
- Chapter 3 describes how to use DirX Identity Manager.
- Chapter 4 describes how to use DirX Identity Server Admin to monitor and manage DirX Identity servers configured in a high availability scenario.
- Chapter 5 describes how you can administer the DirX Identity Java-based server through Web interfaces.
- Chapter 6 provides information about the DirX Identity utilities necessary for data management.
- Appendix A provides information about features that still works but should no longer be used because better features are available

DirX Identity Documentation Set

The DirX Identity document set consists of the following manuals:

- *DirX Identity Introduction*. Use this book to obtain a description of DirX Identity architecture and components.
- *DirX Identity Release Notes*. Use this book to understand the features and limitations of the current release. This document is shipped with the DirX Identity installation as the file **release-notes.pdf**.
- *DirX Identity History of Changes*. Use this book to understand the features of previous releases. This document is shipped with the DirX Identity installation as the file **history-of-changes.pdf**.
- *DirX Identity Tutorial*. Use this book to get familiar quickly with your DirX Identity installation.
- *DirX Identity Provisioning Administration Guide*. Use this book to obtain a description of DirX Identity provisioning architecture and components and to understand the basic tasks of DirX Identity provisioning administration using DirX Identity Manager.
- *DirX Identity Connectivity Administration Guide*. Use this book to obtain a description of DirX Identity connectivity architecture and components and to understand the basic tasks of DirX Identity connectivity administration using DirX Identity Manager.
- *DirX Identity User Interfaces Guide*. Use this book to obtain a description of the user interfaces provided with DirX Identity.
- *DirX Identity Application Development Guide*. Use this book to obtain information how to extend DirX Identity and to use the default applications.
- *DirX Identity Customization Guide*. Use this book to customize your DirX Identity environment.
- *DirX Identity Integration Framework*. Use this book to understand the DirX Identity framework and to obtain a description how to extend DirX Identity.
- *DirX Identity Web Center Reference*. Use this book to obtain reference information about the DirX Identity Web Center.
- *DirX Identity Web Center Customization Guide*. Use this book to obtain information how to customize the DirX Identity Web Center.
- *DirX Identity Meta Controller Reference*. Use this book to obtain reference information about the DirX Identity meta controller and its associated command-line programs and files.
- *DirX Identity Connectivity Reference*. Use this book to obtain reference information about the DirX Identity agent programs, scripts, and files.
- *DirX Identity Troubleshooting Guide*. Use this book to track down and solve problems in your DirX Identity installation.
- *DirX Identity Installation Guide*. Use this book to install DirX Identity.
- *DirX Identity Migration Guide*. Use this book to migrate from previous versions.

Notation Conventions

Boldface type
In command syntax, bold words and characters represent commands or keywords that must be entered exactly as shown.

In examples, bold words and characters represent user input.

Italic type
In command syntax, italic words and characters represent placeholders for information that you must supply.

[ ]
In command syntax, square braces enclose optional items.

{ }
In command syntax, braces enclose a list from which you must choose one item.

In Tcl syntax, you must actually type in the braces, which will appear in boldface type.

|
In command syntax, the vertical bar separates items in a list of choices.

...
In command syntax, ellipses indicate that the previous item can be repeated.

userID_home_directory
The exact name of the home directory. The default home directory is the home directory of the specified UNIX user, who is logged in on UNIX systems. In this manual, the home pathname is represented by the notation *userID_home_directory*.

install_path
The exact name of the root of the directory where DirX Identity programs and files are installed. The default installation directory is *userID_home_directory*/**DirX Identity** on UNIX systems and **C:\Program Files\DirX\Identity** on Windows systems. During installation the installation directory can be specified. In this manual, the installation-specific portion of pathnames is represented by the notation *install_path*.

dirx_install_path
The exact name of the root of the directory where DirX programs and files are installed. The default installation directory is *userID_home_directory*/**DirX** on UNIX systems and **C:\Program Files\DirX** on Windows systems. During installation the installation directory can be specified. In this manual, the installation-specific portion of pathname is represented by the notation *dirx_install_path*.

dxi_java_home
The exact name of the root directory of the Java environment for DirX Identity. This location is specified while installing the product. For details see the sections "Installation" and "The Java for DirX Identity".

tmp_path

The exact name of the tmp directory. The default tmp directory is /tmp on UNIX systems. In this manual, the tmp pathname is represented by the notation *tmp_path*.

tomcat_install_path
The exact name of the root of the directory where Apache Tomcat programs and files are installed. This location is defined during product installation.

mount_point
The mount point for DVD device (for example, **/cdrom/cdrom0**).

1. Using DirX Identity Web Center

Identity **Web Center** is a set of applications that supply identity management functions for use on the web. The applications run on Apache Tomcat and can be accessed by standard Internet browsers.

The DirX Identity product offers two separately licensable versions of Web Center:

- A full-function version that provides the complete set of self-service and management features for end users and administrators.
- A "password management" version that provides a specialized subset of services that allows end users and service desk members to change end user passwords.

Both versions of the Web Center application are delivered with a default configuration so that they can be used right away.

This chapter describes the features and services delivered with the full Web Center package, including general information about:

- Configuring Web Center
- The Web Center page layout
- How to start and log in to Web Center
- Using details pages

This chapter also provides information on how to use the following Web Center services:

- Self Service - permits you to modify your own user data and subscription of services.
- Delegation - allows you to display and delegate your access rights. DirX Identity currently provides an older and a newer implementation and supports them both.
- Work List - allows you to handle approval and certification tasks.
- User Management - allows you to display and manage other users' data.
- Role Management - allows you to display and manage roles.
- Permission Management - allows you to display and manage permissions.
- Group Management - allows you to display and manage groups.
- Account Management - allows you to display and manage accounts.
- Rule Management - allows you to display and manage provisioning rules and password policies.
- Tools - allows you manage reports.
- Help - opens a help file in a separate browser window.
- Logout - allows you to log out from Web Center.
- Business Object Management - allows you to manage business objects.

The chapter "Web Center for Password Management" describes the specific features and

functions provided with the "password management" version of Web Center.

1.1. Configuring Web Center

The topics in this section describe Web Center configuration options, including information about:

- Using the Web Center configuration file **web.xml**
- Configuring Web Center bind passwords
- Configuring single sign-on
- Configuring heap size
- Setting the default language

1.1.1. Using the Web Center Configuration File

The DirX Identity configurator normally sets login parameters. You should use it to change the relevant parameters at any time.

You can also use the **web.xml** configuration file to configure the most important parameters for Web Center by hand. The pathname is:

*install_path***web****webCenter-***domain****webCenter****WEB-INF****web.xml**

The following sections describe the most important **web.xml** parameters. For detailed descriptions of all **web.xml** parameters, see the section "Deployment Descriptor web.xml" in the *DirX Identity Web Center Reference*.

1.1.1.1. Login Parameters

You can set the following login parameters in the Login Parameters section (these parameters are set by the DirX Identity configurator):

- **com.siemens.webMgr.ldap.anyone** - the user that is used for self-registration workflows (Provisioning Configuration). This user has fixed access rights defined by access policies.
- **com.siemens.webMgr.ldap.baseDN** - the base DN to access the domain (for example, "cn=My-Company").
- **com.siemens.webMgr.ldap.host** - the name of the server that contains the Identity Store (Provisioning Configuration).
- **com.siemens.webMgr.ldap.port** - the port of the server that contains the Identity Store (Provisioning Configuration) (per default 389).
- **com.siemens.webMgr.ldap.ssl** (**false**) - the switch that allows accessing the Identity Store (Provisioning Configuration) via SSL.
- **com.siemens.webMgr.ldap.user** - the technical user that is used to access the Identity Store (Provisioning Configuration). The specific user's access rights are calculated by access policies.

For example, you may want to set the Login parameter section to the correct parameters for your customer domain.

1.1.1.2. Request Workflow Service Parameters

This section comprises parameters for the connection from Web Center to the request workflow service.

- **com.siemens.webMgr.requestworkflow.keystoreName** - the location of the key store for single sign-on from Web Center to the request workflow server.
- **com.siemens.webMgr.requestworkflow.keyAlias (WebCenter)** - the alias of the key entry in this key store.
- **com.siemens.webMgr.requestworkflow.updateTimeout (0)** - the amount of time (in milliseconds) to wait for a response from the request workflow engine (for example, the list of allowed workflows or the next activity to be performed).

1.1.1.3. Session Configuration

This section comprises standard configuration parameters for session handling:

- **session-timeout** - the time (in minutes) after which the session for a logged in user times out if no action is taken.
- **tracking-mode** - the way in which the browser sends the session ID to the server with each request. For security reasons, we strongly recommend setting the mode to **COOKIE**.

1.1.1.4. Log Level Parameters

- **com.siemens.webMgr.log.level** - allows you to set the amount of logging for the Web Center application:
  -1 - OFF: disables logging
  -2 - Uses the log4j configuration file **WEB-INF/classes/log4j.properties**
  0 - SEVERE: displays only severe errors
  1 - INFO: displays additional information
  2 - FINEST: shows the most detailed level of information (this selection can be useful for viewing JMS message content or for performing Struts debugging).

1.1.2. Configuring Web Center Bind Passwords

Web Center must perform a login to the Identity Store as part of a user login. The necessary passwords for this action must be present in the Web Center configuration file. Web Center can read passwords in clear text or in encrypted format.

If you enter a password in clear text, the server reads it during the next startup, encrypts it and writes it back to the configuration file. From now on, the password information is no longer readable. If you are in doubt that the right password is set or if you need to set a new password, simply replace the encrypted value with the clear text value. During the next Web Center startup, the server will encrypt the new password (or pin value).

You can set the passwords in the file:

install_path\web\webCenter-***domain***\webCenter\WEB-INF\password.properties*

This file contains the following passwords:

ldap - the technical password used by Web Center for all accesses. The individual accesses of users are protected via access policies. For details about access policies, see the *DirX Identity Provisioning Administration Guide*.

ANYONE - the password used for self-registration processes with restricted functionality.

pin - the PIN for the private key used to encrypt passwords.

previousPin - the PIN for the private key previously used to encrypt passwords.

1.1.3. Configuring Challenge/Response Authentications

This section describes how to set up challenge/response authentications in Web Center.

1.1.3.1. Configuring Challenge Proposal Lists

A proposal list is a set of predefined questions from which users can select when editing their authentication questions. You can define a proposal list for each language that Web Center supports. If there is no proposal list defined for a specific language, Web Center uses the default list.

The proposed questions for one language are independent of the questions for another language and the number of questions can vary with each language. The following example shows a set of four English questions, while the German set includes only three questions.

Language “en“

- My PIN
- My favorite DNA sequence
- My favorite random number
- My favorite response

Language “de”

- Meine PIN
- Meine Lieblings-DNS-Sequenz
- Mein Lieblingstier

In its simplest form, a proposal defines the text of the question displayed in Web Center whenever a user edits his authentication questions or attempts to authenticate via challenge/response. When editing, the proposed questions are available for selection in the section “Questions from Proposal List“. Questions that have previously been answered are

also displayed in this section, provided they match one of the proposed questions. If not, they are displayed in section “Other Questions“. The latter case occurs not only for free text questions but also for questions selected from a proposal list for a different language.

1.1.3.2. Identifying Questions from Different Languages

In the above example, the English question “My PIN“ is considered to be different from the German question “Meine PIN“ although both questions are just translations of the same question.

Suppose a user edits his questions in English and defines an answer for “My PIN”. Later on, he edits his questions again, this time in German. Question “My PIN” is then shown in section “Other Questions” while the proposal list section allows selecting “Meine PIN”. The user could then enter a different answer for “Meine PIN” than for “My PIN”.

Usually, however, both questions are considered identical and should just specify different labels for the same question. A response assigned to “My PIN” should be also a response to “Meine PIN”, and vice versa.

You can achieve this by assigning the same key to both questions, for example, the key “PIN”:

Language “en“

- PIN;My PIN
- DNA;My favorite DNA sequence
- My favorite random number
- My favorite response

Language “de”

- PIN;Meine PIN
- DNA;Meine Lieblings-DNS-Sequenz
- Mein Lieblingstier

Separate the key and label with a semicolon (;). Assign the key to the corresponding label in each proposal list containing the question.

1.1.3.3. Defining Mandatory Questions

You can mark one or more questions from a proposal list as mandatory. Users must then define answers to these questions when editing their authentication questions. And if a user attempts to authenticate via challenge/response, s/he must give the correct answers to all mandatory questions.

A question marked as mandatory for one language must also be marked as mandatory for all other languages. Otherwise a user having entered the mandatory questions for one language might fail to authenticate in a different language since he hasn’t answered the mandatory questions for this language. Or he might be able to authenticate in another

language without answering mandatory questions if the other language has no mandatory questions defined. Issues might also arise when editing authentication questions in different languages with different sets of mandatory questions.

A question is mandatory if its key starts with “Mandatory-”. For example:

Language “en”

- Mandatory-PIN;My PIN
- DNA;My favorite DNA sequence
- My favorite random number
- My favorite response

Language “de”

- Mandatory-PIN;Meine PIN
- DNA;Meine Lieblings-DNS-Sequenz
- Mein Lieblingstier

If a service desk member is asked by a user to reset his password (via Web Center for Password Management), he usually checks the user’s identity by asking him to give the answers to one or more of his authentication questions. In this case, Web Center for Password Management indicates to the service desk member which questions are mandatory. The service desk member, however, can decide whether the questions must be answered for a successful identification.

1.1.3.4. Relevant DirX Identity Manager Objects

In DirX Identity Manager, open the **Provisioning** view → **Domain Configuration** and change to folder **Customer Extensions** → **Proposal Lists** → **Nationalization** → **Challenges**. This folder contains a proposal list for each supported language. The name of a proposal list is identical to the corresponding language name (like **en** or **de**), or to language and country name (like **en_US** or **de_AT**).

Each proposal list is of type String and specifies the proposed questions in **Proposed Values**.

The default language can be assigned to **Default Language** in the **Challenges** folder.

1.1.3.5. Other Configuration Options

You can customize challenge/response in the file **webCenter.properties** by changing the following parameters:

- **editableChallenges** - Allow (**true**) or prohibit (**false**) free text questions. Default: **true**.
- **minEnteredChallenges** - The minimum number of questions to define and answer. Default: **6**.
- **challengeResponses.minimumResponseLength** - The minimum response length.

Default: no minimum length.

- **challengeResponses.duplicateResponsesAllowed** - Allow (**true**) or prohibit (**false**) identical answers to different questions. Default: **true**.
- **challengeResponses.trimOnAnswering** - Whether to remove (**true**) leading and trailing white spaces from responses during challenge/response authentication. Default: **true**.
- **challengeResponses.trimOnEditing** - Whether to remove (**true**) leading and trailing white spaces from free text questions and responses when editing authentication questions. Default: **true**.

1.1.4. Configuring Single Sign-on

DirX Identity Web Center can use single sign-on (SSO) methods to authenticate users. In addition to the usual DirX Identity default authentication, the Web Center supports the following single sign-on methods:

- Authentication via HTTP header, providing either
- A target system domain and account that uniquely identifies a user
- An attribute value uniquely identifying a user
- A user's distinguished name

HTTP header authentication subsumes authentication with a user certificate and via a request-scoped attribute (instead of an HTTP header).

- Windows single sign-on via the SPNEGO authentication module
- SAP logon ticket

A single sign-on request is first processed by one or more modules that extract the user credentials from the request and optionally validate the credentials.

On success, the request is forwarded to the Web Center authentication module which maps the credentials to a DirX Identity user identity used for control decisions in subsequent operations. The following figure illustrates the process.

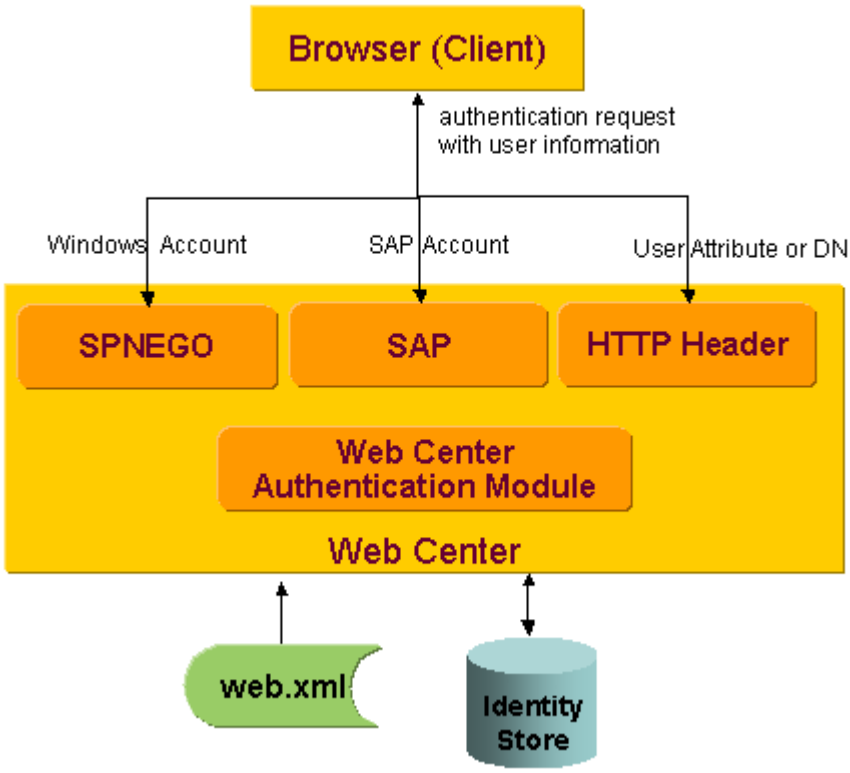

Figure 1. Performing Single Sign-On

As shown in the figure, Web Center checks an incoming authentication request against local configuration information contained in the configuration file **web.xml** to determine if the authentication request matches the pre-requisites for single sign-on specified in the file. Web Center then authenticates the request locally according to the DirX Identity default authentication procedure - by checking the credentials transmitted in the authentication request against the DirX Identity store - or forwards the user information to the corresponding internal authentication module. Web center maps the user information onto the DirX Identity user identity after successful single sign-on authentication.

The following sections describe the supported methods and how to configure them.

When using single sign-on, you must set up the connection from Web Center to the request workflow server (a component of the Java-based server) for single sign-on as well. (See the *DirX Identity Web Center Reference* for details.)

1.1.4.1. About the Web Center Authentication Module

This section provides an overview of the configuration options and the resolution algorithms of the Web Center authentication module.

1.1.4.1.1. Configuration Options

To perform single sign-on authentication specify the following context initialization parameters in the configuration file **web.xml**.

General LDAP Parameters

The names of the general LDAP parameters start with the prefix **com.siemens.webMgr.ldap.** DirX Identity automatically assigns the appropriate values while performing initial configuration. The following table lists the relevant general LDAP parameters:

Parameter Name	Default	Description
baseDN	cn=My-Company	General LDAP search base for DirX Identity Provisioning

Module-Specific Parameters

The names of the SSO module specific parameters start with the prefix **com.siemens.webMgr.auth.** The following table lists the parameters:

Parameter Name	Default	Description
varName	com.siemens.webMgr.ssoUserInfo	Session-scoped variable name of the credentials
userBase	cn=Users,*LDAP_search_base*	Search base for user entries
userFilter	(&(objectclass=dxrUser)(sn=%USER_ID))	Search filter for user entries
targetSystemBase	cn=TargetSystems,*LDAP_search_base*	Search base for target system entries
targetSystemFilter	(&(objectclass=dxrTargetSystem) (dxrTSDomainName=%DOMAIN))	Search filter for target system entries
accountFilter	(&(objectclass=dxrTargetSystemAccount) (dxmADsSamAccountName=%ACCOUNT))	Search filter for account entries
accountUserLink	dxrUserLink	Attribute name of the attribute storing the user's DN in an account entry

1.1.4.1.2. Resolution Algorithm

The Web Center authentication module uses the SSO credentials from the session-scoped variable to find a matching user in the DirX Identity database. The module supports the following resolution algorithms:

- Find a user with a given DN.

- Find a user that matches a given user attribute value.
- Find a user that is linked to a given account in a given target system.

The first two options only differ in the configuration options.

Resolution Algorithm with Given DN or Attribute Value

The Web Center authentication module performs the following steps:

1. Reads the templates for user search base and filter from the configuration file **web.xml** and replaces all occurrences of %USER_ID in both templates with the given user DN or attribute value.
2. Performs a search in the DirX Identity store below the resulting search base with the resulting filter.
3. If the search returns exactly one user, the authentication module returns success and the user's DN; otherwise, it returns an error.

The following figure illustrates this resolution algorithm.

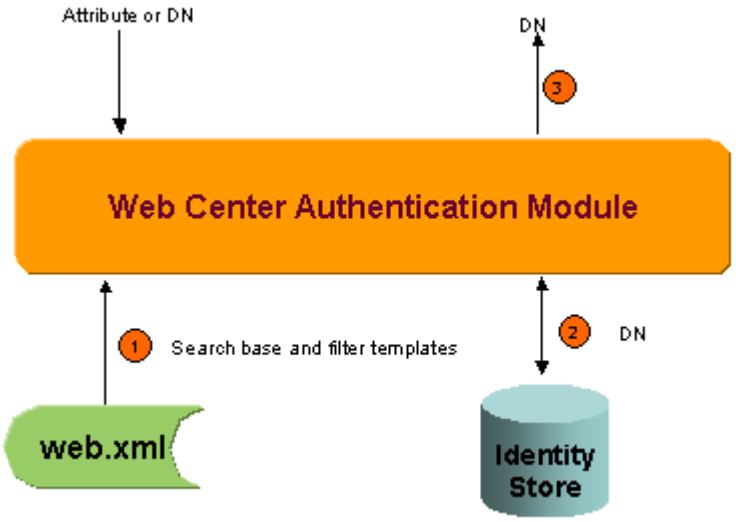

Figure 2. Resolution Algorithm with given DN or Attribute Value

Resolution Algorithm with Target System and Account

The Web Center authentication module performs the following steps:

1. Reads the templates for target system search base and filter from the configuration file **web.xml** and replaces all occurrences of %ACCOUNT, %DOMAIN, and %CLIENT in both templates with the specified account, domain, and client values.
2. Performs a search in the DirX Identity store below the resulting search base with the resulting filter.
3. If the search returns exactly one target system, the authentication module reads the account filter template from the configuration file **web.xml** and replaces all occurrences of %ACCOUNT, %DOMAIN, and %CLIENT in the template with the specified account, domain, and client values; otherwise, it returns an error.

4. Performs a search in the DirX Identity store below the target system found in step 2 with the resulting filter.
5. If the search returns exactly one account, the authentication module reads the attribute name that links accounts to their users from the configuration file **web.xml**; otherwise, it returns an error.
6. Reads the attribute value (a user DN) of the account found in step 4.
7. On success, the authentication module returns the user DN; otherwise, it returns an error.

The following figure illustrates this resolution algorithm.

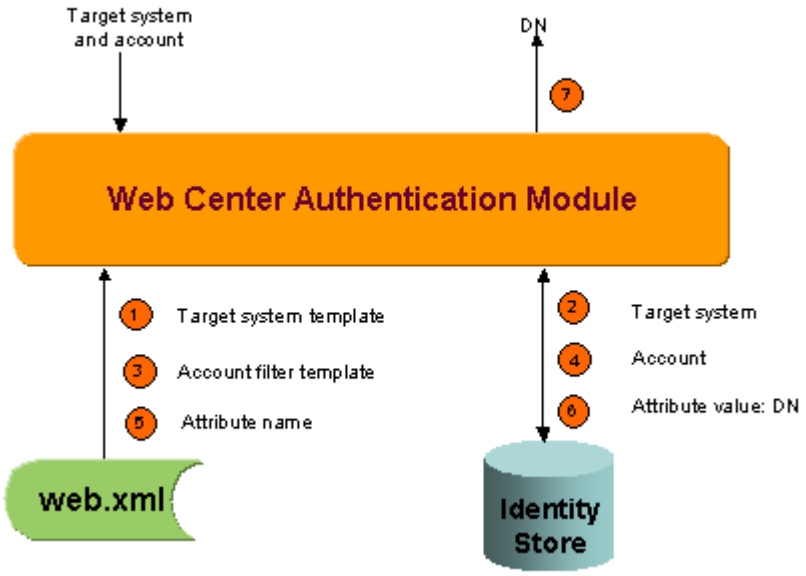

Figure 3. Resolution Algorithm with Target System and Account

1.1.4.2. Using SSOHeaderFilter

The SSOHeaderFilter is a servlet filter that extracts SSO credentials from an HTTP header and stores them in a session-scoped variable.

The filter can act as a stand-alone SSO module in case the client provides unencrypted credentials via an HTTP header. Its other purpose is to copy credentials provided by another SSO module (for example, a Tomcat valve) to session-scope.

Note that the filter does not validate the source of the credentials. As a result, deploying it as a stand-alone SSO module may cause a security breach if untrusted clients can access WebCenter directly.

1.1.4.2.1. Filter Definition

The filter definition must be inserted in the configuration file **web.xml** after the **SessionFilter** definition as follows:

```
<!-- SSO header filter definition -->
<filter>
     <filter-name>
               SSOHeaderFilter
</filter-name>
<display-name>
   SSO Header Filter
</display-name>
<description
    Evaluates single sign-on information passed in HTTP headers
</description>
<filter-class>
   com.siemens.webMgr.filter.SSOHeaderFilter
</filter-class>
Initialization parameters
<filter>
```

1.1.4.2.2. Initialization Parameters

The following table lists the initialization parameters:

Parameter Name	Default	Description
headerName	none	HTTP header name, or name of a request-scoped variable Required
authType	none	Expected authorization type (for example, **BASIC**)
type	account	Type of credentials: **user** or **account**
userRegExpr	(.*)	Regular expression to extract the user attribute value or DN from the header value Not relevant for type **account**
domainRegExpr	[^@]*@(.*)	Regular expression to extract the domain from the header value Not relevant for type **user**
clientRegExpr	-	Regular expression to extract the client from the header value Not relevant for type **user**

Parameter Name	Default	Description
accountRegExpr	([^@]*)@.*	Regular expression to extract the account from the header value Not relevant for type **user**
varName	com.siemens.webMgr.ssoUserInfo	Session-scoped variable name of the credentials

1.1.4.2.3. Notes

This section provides information about SSOHeaderFilter operation.

headerName

The header or variable value is obtained as follows:

- If the header name is **UserPrincipal**:
  Call **request.getUserPrincipal().getName()**.
- If the header name is Authorization or RemoteUser:
  Call request.getRemoteUser().
- If the header name starts with ClientCertificate.:
  Call request.getAttribute("javax.servlet.request.X509Certificate") to get the certificate and extract the data identifying a user from the certificate as described below.
- Otherwise, call request.getHeader(<headerName>). If the header value is empty, call request.getAttribute(<headerName>).

To extract data from a certificate, the filter proceeds as follows:

- If the header name starts with **ClientCertificate.Principal.**:
  Call **cert.getSubjectX500Principal()** to get the principal DN and extract data from the DN as described below.
- If the header name starts with **ClientCertificate.AltName.DirectoryName.**:
  Get the directory name from the certificate subject's alternative names and extract data from the DN as described below.
- If the header name is **ClientCertificate.AltName.rfc822Name**:
  Get the mail address from the certificate subject's alternative names.

To extract data from a certificate subject's DN, the filter proceeds as follows:

- If the header name ends with **dn**:
  Take the entire DN as value.
- If the header name ends with **rdn**:
  Take the attribute value of the last RDN as value.
- If the header name ends with **<RDN attribute type>**:
  Take the attribute value of the last RDN with that attribute type as value.

Header name comparison is done ignoring case.

authType

The current authorization type is obtained by calling **request.getAuthType()**. If an authorization type is not configured, the current type is arbitrary and may be missing.

userRegExpr

The default expression extracts the entire header value.

domainRegExpr and accountRegExpr

The default expressions are suited for header values in the format *account**@**domain*.

Regular Expressions

For the syntax of regular expressions, refer to the API specification of the standard Java package **java.util.regex**.

Filter Mapping

The filter must be mapped to the URL pattern ***.do** and ***.jsp**. The mappings must be inserted in the configuration file **web.xml** after the **SessionFilter** mappings.

```
<!-- SSOHeaderFilter mappings -->
<filter-mapping>
   <filter-name>SSOHeaderFilter</filter-name>
   <url-pattern>*.do</url-pattern>
<filter-mapping>
<filter-mapping>
   <filter-name>SSOHeaderFilter</filter-name>
   <url-pattern>*.jsp</url-pattern>
<filter-mapping>
<filter-mapping>
   <filter-name>SSOHeaderFilter</filter-name>
   <url-pattern/saveFile</url-pattern>
<filter-mapping>
```

1.1.4.3. Authentication via HTTP Header

This section provides information about the authentication process via HTTP header.

1.1.4.3.1. Authentication Process with User Attribute

This section provides information on how to administer the configuration file **web.xml** when performing authentication with a user attribute in the HTTP header and how the authentication is processed.

SSOHeaderFilter Configuration

For configuring the SSOHeaderFilter, the following rules apply:

- The header name is use case specific.
- The credential type is **user**.
- All other parameters are not relevant or can be left to their default values.

Example:

When the header name is **SCGID** the configuration is as follows:

```
<init-param>
     <param-name>headerName</param-name>
     <param-value>SCGID</param-value>
</init-param>
<init-param>
     <param-name>type</param-name>
     <param-value>user</param-value>
</init-param>
```

Web Center Authentication Module Configuration

For configuring the Web Center authentication module, the following rules apply:

- The attribute name in the user filter must be set to the appropriate value.
- All other parameters are either not relevant or can be left to their default values.

When the attribute name is **gid** the configuration is as follows:

```
<context-param>
   <param-name>
       com.siemens.webMgr.auth.userFilter
   </param-name>
   <param-value>
      (&amp;(objectclass=dxrUser)(gid=%USER_ID))
   </param-value>

</context-param>
```

Authentication Process

The following figure illustrates the authentication process with a user attribute given in the HTTP header identifying the user.

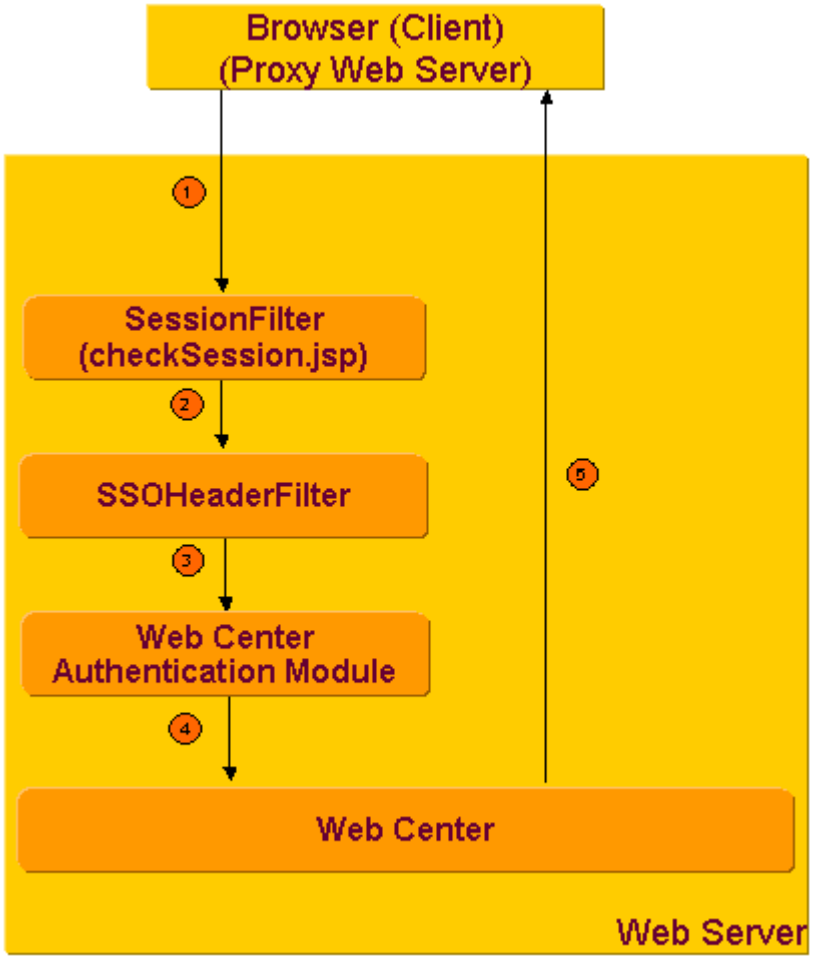

Figure 4. HTTP Header Single Sign-on Authentication Process with User Attribute

As illustrated in the figure:

1. The browser sends a request that includes an HTTP header with a user attribute value, for example, a unique user id. In real life, the header is usually not set by the browser directly. Instead, the request is preprocessed by a proxy web server that authenticates the client and adds the header to the request.
2. The SessionFilter preprocesses the request to check for invalid session cookies.
3. The SSOHeaderFilter extracts the attribute value from the header and copies it to session-scope.
4. The Web Center authentication module searches for a DirX Identity user matching the attribute value, and skips the login page. Note that the module is not called if the session already includes DirX Identity login data from a previous request. In this case, the new request is processed on behalf of the DirX Identity user stored in the session.
5. If a matching user is found, the request is processed and the appropriate page is returned to the browser. Otherwise, Web Center displays its login page and prompts the client to log in.

Security

The SSOHeaderFilter does not validate the source of the header value, which causes a security breach if untrusted clients can access Web Center directly. Direct access to Web Center should, for instance, be restricted to the proxy server generating the header.

1.1.4.3.2. Authentication Process with User DN

This section provides information on how to administer the configuration file **web.xml** when performing authentication with a user DN in the HTTP header and how the authentication is processed.

SSOHeaderFilter Configuration

For configuring the SSOHeaderFilter, the following rules apply:

- The header name is use case specific.
- The credential type is **user**.
- All other parameters are not relevant or can be left to their default values.

Example:

For HTTP basic authentication with DN and password, the configuration is as follows:

```
<init-param>
     <param-name>authType</param-name>
     <param-value>BASIC</param-value>
</init-param>
<init-param>
     <param-name>headerName</param-name>
     <param-value>Authorization</param-value>
</init-param>
<init-param>
       <param-name>type</param-name>
       <param-value>user</param-value>
</init-param>
```

Web Center Authentication Module Configuration

For configuring the Web Center authentication module, the following rules apply:

- The user search base is the supplied user DN.
- The user search filter is just **(objectclass=dxrUser)**.
- All other parameters are either not relevant or can be left to their default values.

```
<context-param>
   <param-name>
```

```
        com.siemens.webMgr.auth.userBase</param-name>
    <param-value>%USER_ID</param-value>
</context-param>
<context-param>
    <param-name>
        com.siemens.webMgr.auth.userFilter
    </param-name>
         <param-value>(objectclass=dxrUser)</param-value>
</context-param>
```

Authentication Process

The following figure illustrates the authentication process for HTTP basic authentication with user DN.

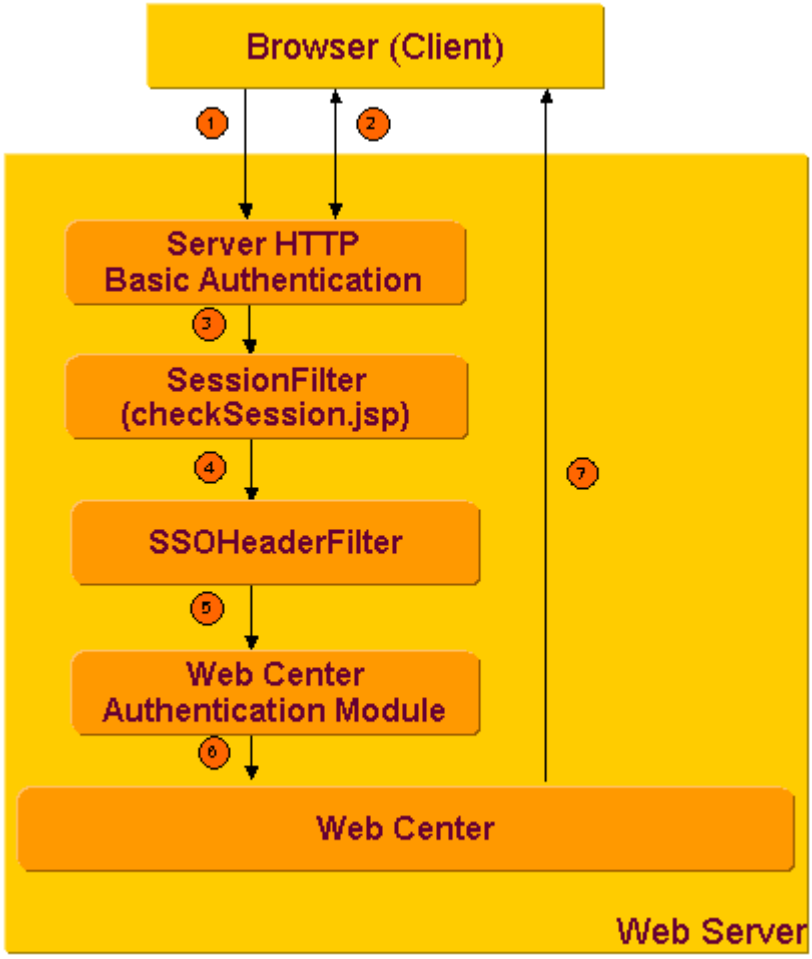

Figure 5. HTTP Header Single Sign-on Authentication Process with User DN

As illustrated in the figure:

1. The browser sends a request to Web Center.

2. Web Center is configured to require HTTP basic authentication. Therefore, the web server handles the necessary protocol to get and validate the client credentials.
3. The credentials, in this case the user's DN, are stored in the HTTP Authorization header.
4. The SessionFilter preprocesses the request to check for invalid session cookies.
5. The SSOHeaderFilter extracts the DN from the header and copies it to session-scope.
6. The Web Center authentication module searches for a DirX Identity user with the given DN, and skips the login page. Note that the module is not called if the session already includes DirX Identity login data from a previous request. In this case, the new request is processed on behalf of the DirX Identity user stored in the session.
7. If a matching user is found, the request is processed and the appropriate page is returned to the browser. Otherwise, Web Center displays its login page and prompts the client to log in.

Security

The solution is secure because each request to Web Center must pass through Tomcat's HTTP basic authentication module which sets the header. HTTPS must be used to prevent clear text passwords being transmitted over the network.

1.1.4.4. Windows Single Sign-On via SPNEGO

This section provides information about Windows single sign-on authentication via Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO). The first part provides information about the configuration data that must be specified in the configuration file **web.xml**. The second part provides information about the authentication process.

See the appendix "Windows SSO" in the *DirX Identity Installation Guide* for instructions on how to install and set up Windows single sign-on.

1.1.4.4.1. Authentication Process

This section provides information on how to administer the configuration file **web.xml** when performing Windows single sign-on via SPNEGO and how the authentication is processed.

SSOHeaderFilter Configuration

For configuring the SSOHeaderFilter, the following rules apply:

- The combined **<account>@<domain>** value must be obtained from the Authorization header via **request.getRemoteUser ()**.
- The expected authorization type is **SPNEGO/Kerberos**.
- All other parameters are not relevant or can be left to their default values.

```
<init-param>
    <param-name>headerName</param-name>
    <param-value>RemoteUser</param-value>
```

```
</init-param>
<init-param>
    <param-name>authType</param-name>
    <param-value>SPNEGO/Kerberos</param-value>
</init-param>
```

Web Center Authentication Module Configuration

The SPNEGO authentication method is the default case for the authentication module. Therefore, all parameters are either not relevant or can be left to their default values.

Authentication Process

The following figure illustrates the authentication process via SPNEGO.

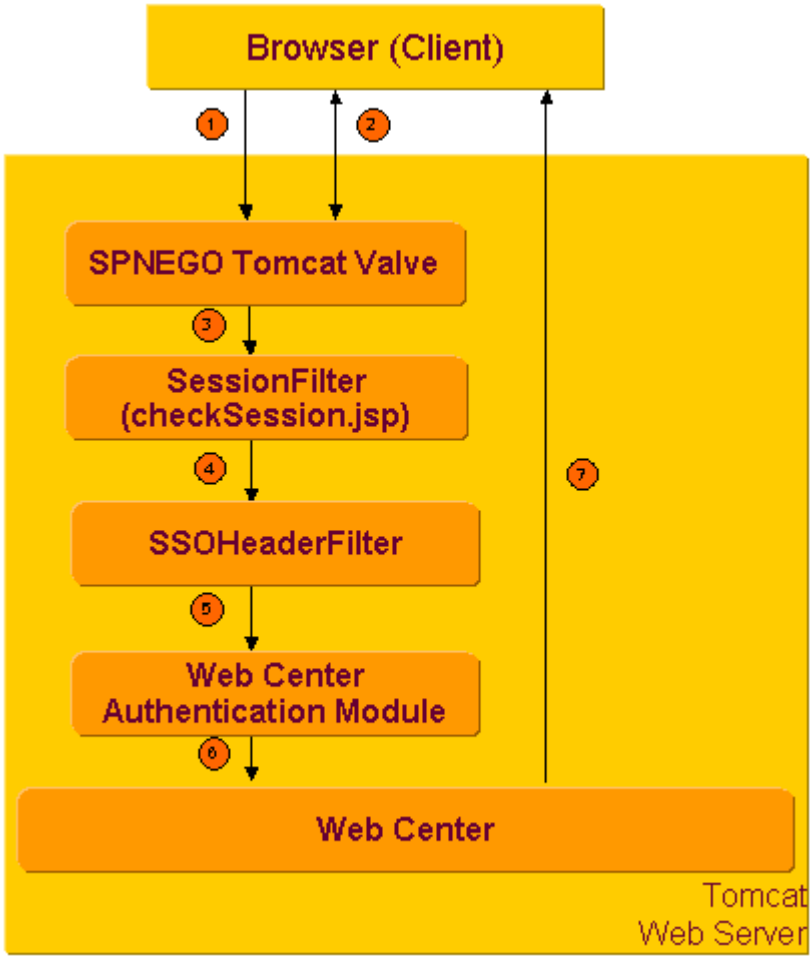

Figure 6. Windows Single Sign-on Authentication Process with SPNEGO

As illustrated in the figure:

1. The browser sends a request to Web Center.
2. Web Center is configured to require SPNEGO authentication; as a result, the SPNEGO

Tomcat valve handles the proper protocol to get and validate the client credentials.

3. The credentials, in this case the user's Windows account and Windows domain name, are stored in the HTTP Authorization header.
4. The SessionFilter preprocesses the request to check for invalid session cookies.
5. The SSOHeaderFilter extracts account and domain from the header and copies them to session-scope.
6. The Web Center authentication module searches for a DirX Identity user associated with the given account in the given domain, and skips the login page. Note that the module is not called if the session already includes DirX Identity login data from a previous request. In this case, the new request is processed on behalf of the DirX Identity user stored in the session.
7. If a matching user is found, the request is processed and the appropriate page is returned to the browser. Otherwise, Web Center displays its login page and prompts the client to log in.

Security

The solution is secure because each request to Web Center must pass through the SPNEGO valve which runs in the Tomcat web server.

1.1.4.5. Authentication via User Certificate

A user may authenticate to Web Center with his certificate. The authentication process involves the following steps:

- The user starts Web Center in his browser.
- As Web Center is configured to require client certificate authentication, Tomcat asks the client to identify accordingly.
- The browser gets the requested credentials from its certificate store or a card reader and sends them to the server. During this step, the browser may ask the user to enter a PIN or password required to read the credentials.
- Tomcat verifies the presented certificate. For this action, Tomcat's trust store must contain the presented certificate or one of the certificates in its certification path.
- Tomcat assigns the certificate to the request-scoped variable **javax.servlet.request.X509Certificate**, and forwards request processing to Web Center.
- The SSOHeaderFilter extracts data identifying the user from the certificate and sets the session-scoped variable **com.siemens.webMgr.ssoUserInfo** accordingly.
- The Web Center login procedure maps the data to a user in the DirX Identity database.

Note that the authentication only works with HTTPS.

1.1.4.5.1. Configuring User Certificate Authentication

When finished, restart Tomcat, and don't forget to put a card into the reader.

Setting up Key Store and Trust Store for Tomcat

Use the Java keytool utility to perform the following tasks:

- Create a key store with a private key for Tomcat.
- Create a trust store for Tomcat and import the certificate of any certificate authority that's in the certification path of every user's certificate into the trust store (or add every user's certificate).

Configuring Tomcat

In the file **TOMCAT_HOME/conf/server.xml**, go to the SSL connector definition, add key store and trust store attributes and change the **clientAuth** attribute:

```
<Connector port=”8443” ...
    clientAuth="want"
    keystorePass="<keystore password>"
    keystoreFile="<full path name of keystore file>"
    truststorePass="<truststore password>"
    truststoreFile="<full path name of truststore file>" .../>
```

Configuring Web Center SSO Handlers

To configure the Web Center SSO handlers:

- Activate the **SSOHeaderFilter** and set the value for its initialization parameter **headerName**, for example:

```
<filter>
     <filter-name>SSOHeaderFilter</filter-name>
     ...
     <init-param>
             <param-name>headerName</param-name>
             <param-value>ClientCertificate.Principal.RDN</param-
value>
     </init-param>
     ...
</filter>
```

- Activate the filter mappings for the **SSOHeaderFilter**.
- Activate and set a user filter context parameter, for example:

```
<context-param>
    <param-name>com.siemens.webMgr.auth.userFilter</param-name>
```

```
    <param-value>
       (&amp;(objectclass=dxrUser)(cn=%USER_ID))
   </param-value>
</context-param>
```

1.1.4.6. Single Sign-on With DirX Access

This section gives some hints for running Web Center behind a DirX Access PEP.

- Web Center's home page might require re-configuring the CSRF filter in order to work properly. In file **WEB-INF/config/webCenterCustom.properties**, add all actions linked to the home page to the CSRF configuration parameters as in the following sample:

  ```
  # ----------------------------------------------------------------
  # CSRF token
  # ----------------------------------------------------------------
  csrf.allowPostForEntryPoints = true
  csrf.entryPoints = /login.do,/index.jsp,/error.do,/logout.do,\
                     /homeTasks.do,/homeSummary.do,\
                     /homeRoles.do,/homeCampaigns.do
  ```

- This hint applies to DirX Identity versions prior to 8.9 only:

  You might encounter character encoding issues when entering data containing non-ASCII characters. In that case, use a Tomcat filter to inform the server that the character encoding to be used for processing incoming Web Center requests is "UTF-8".

  Add the filter definition to file **WEB-INF/web.xml**:

  ```
  <filter>
     <filter-name>SetCharEncodingFilter</filter-name>
     <filter-class>
         org.apache.catalina.filters.SetCharacterEncodingFilter
     </filter-class>
     <init-param>
         <param-name>encoding</param-name>
         <param-value>UTF-8</param-value>
     </init-param>
  </filter>
  ```

  Map the filter to all incoming requests:

```
<filter-mapping>
   <filter-name>SetCharEncodingFilter</filter-name>
   <url-pattern>/*</url-pattern>
</filter-mapping>
```

Insert the filter mapping before all other filter mappings, including the ones for the DirX Access PEP filter.

- This hint applies to DirX Identity versions prior to 8.6 only:

  Remove jaxws-rt.jar and jaxws-tools.jar from folder **WEB-INF/lib**. Otherwise, access to the request workflow service might fail.

1.1.4.7. Single Sign-on via SAP Logon Ticket

This section provides information about single sign-on authentication with SAP Logon Ticket. The first part provides information about the configuration data that must be specified in the configuration file **web.xml**. The second part provides information about the authentication process.

1.1.4.7.1. SAPSSOFilter

The SAPSSOFilter integrates Web Center into SAP NetWeaver. It is a servlet filter that gets an SAP logon ticket from an HTTP cookie, validates the ticket, and stores the provided credentials in session-scope for further evaluation by the Web Center authentication module.

In addition to evaluating the ticket, the filter checks the following:

- Whether the credentials have changed since the previous request.
- Whether the user's language is specified in the request parameters.

The check results are included in the session-scoped variable for further evaluation by subsequent JSP pages.

Prerequisites

In order to validate the provided credentials, the filter needs a certificate of the ticket-issuing SAP system. The certificate can either be provided in a file or in a key store. The certificate can be easily downloaded from the NetWeaver Portal administration.

The filter also requires that the library **dxmMySap.jar** is copied from *install_path**/web/webManagerForSAP-***domain***/shared* to the **TOMCAT_HOME/lib** folder.

Filter Definition

The filter definition must be inserted in the configuration file **web.xml** after the **SessionFilter** definition as follows:

```
<!-- SAPSSOFilter definition -->
<filter>
   <filter-name>SAPSSOFilter</filter-name>
   <display-name>
       SAP SSO Evaluation Filter
   </display-name>
   <description
       Verifies and evaluates SAP logon tickets
   </description>
   <filter-class>
       com.siemens.webMgr.filter.SAPSSOFilter
   </filter-class>
   Initialization parameters
<filter>
```

Initialization Parameters

The following table lists the initialization parameters:

Parameter Name	Default	Description
certFile	none	Name of certificate file
keyStore	none	Name of key store containing the certificate
keyStorePassword	none	The key store password
certAlias	none	The alias for the certificate in the key store
ssoCookieName	MYSAPSSO2	Name of logon ticket cookie
decoderCharset	ISO-8859-1	Character set for decoding the logon ticket cookie
languageParamName	language	Name of the request parameter providing the user language
varName	com.siemens.webMgr.ssoUserInfo	Name of session-scoped variable for credentials
logLevel	error	Log level: **error** or **debug**

Notes

This section provides information about SAPSSOFilter operation.

certFile

Specify the file name as an absolute path name or relative to Tomcat's current working directory. The file name may start with @CATALINA_BASE@ which is replaced by Tomcat's installation directory at runtime.

keyStore, keyStorePassword, and certAlias

Specify the key store name as an absolute path name or relative to Tomcat's current working directory. The file name may start with @CATALINA_BASE@ which is replaced with Tomcat's installation directory at runtime.

The options are ignored if the certificate can be obtained from the certificate file.

decoderCharset

The value of the logon ticket cookie is URL encoded. The **decoderCharset** option specifies the character set to be used to URL decode the cookie value.

logLevel

The filter uses the logging interface of the Java Servlet API. With Tomcat's default log settings enabled, the output is written to Tomcat's standard output.

Filter Mapping

The filter must be mapped to the URL patterns ***.do** and to the Web Center start page. The mappings must be inserted in the configuration file **web.xml** after the **SessionFilter** mappings.

```
<!-- SAPSSOFilter mappings -->
<filter-mapping>
   <filter-name>SAPSSOFilter</filter-name>
   <url-pattern>*.do</url-pattern>
<filter-mapping>
<filter-mapping>
   <filter-name>SAPSSOFilter</filter-name>
   <url-pattern>/index.jsp</url-pattern>
<filter-mapping>
```

1.1.4.7.2. Authentication Process

This section provides information on how to administer the configuration file **web.xml** when performing single sign-on with SAP Logon ticket and how the authentication is processed.

SAPSSOFilter Configuration

In the simplest case, it is sufficient to specify the certificate file name. The configuration is as follows:

```
<init-param>
   <param-name>certFile</param-name>
   <param-value>
       @CATALINA_BASE@/sap/verify.der
   </param-value>
</init-param>
```

Web Center Authentication Module Configuration

For single sign-on with SAP logon tickets to work, you must

- Assign the name of the ticket-issuing SAP system to the attribute **dxrTSDomainName** of a target system in the DirX Identity store.
- Assign each NetWeaver user login to an attribute of an account below this target system.

The name of the ticket-issuing system is the value of the certificate's issuer field; for example, F31.

If the account attribute name is **sapUsername**, the authentication module configuration is as follows:

```
<context-param>
   <param-name>
       com.siemens.webMgr.auth.accountFilter
   </param-name>
   <param-value>
       (&amp;(objectclass=dxrTargetSystemAccount)
             (sapUsername=%ACCOUNT))
   </param-value>
</context-param>
```

Authentication Process

The following figure illustrates the authentication process with SAP logon ticket.

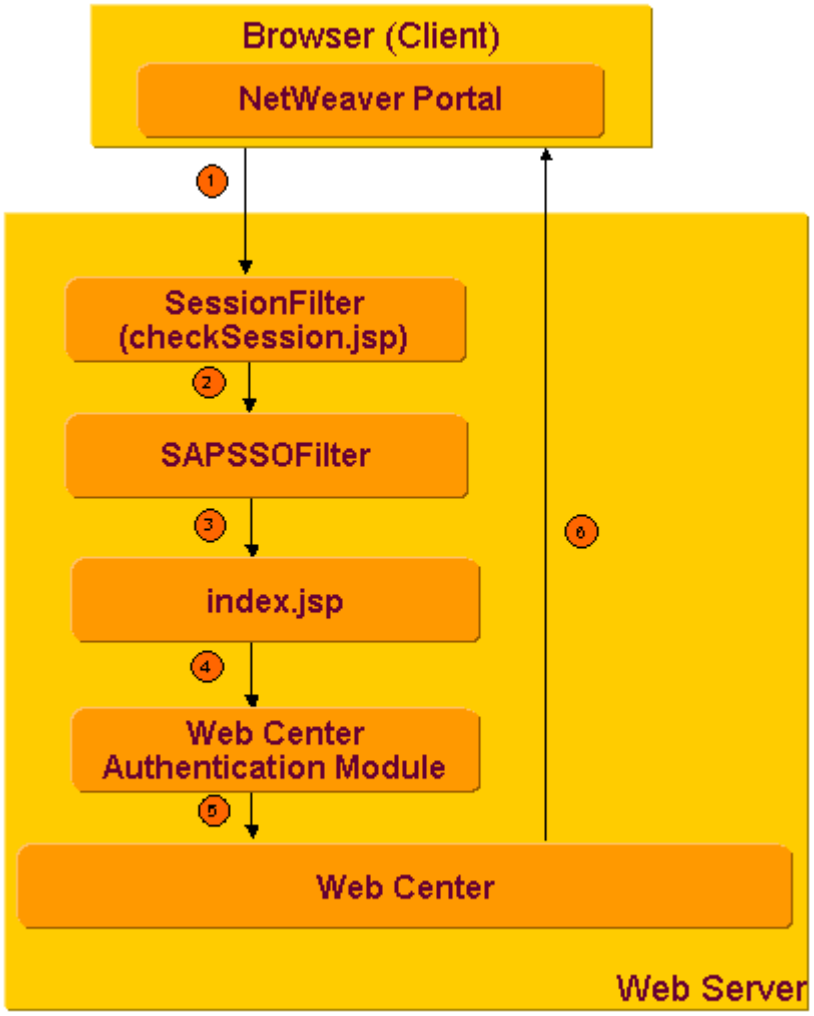

Figure 7. Single Sign-on Authentication Process with SAP Logon Ticket

As illustrated in the figure:

1. NetWeaver sends an HTTP request to Web Center. The request includes the current user's logon ticket in an HTTP cookie. The request may for instance be initiated when the user logs in to NetWeaver, or when he selects a menu item.
2. The SessionFilter preprocesses the request to check for invalid session cookies.
3. The SAPSSOFilter validates the logon ticket and copies the credentials to session-scope.
4. A JSP that checks for inappropriate session cookies preprocesses the request.
5. The Web Center authentication module searches for a DirX Identity user matching the credentials. Note that the module is not called if the session already includes DirX Identity login data from a previous request. In this case, the new request is processed on behalf of the DirX Identity user stored in the session.
6. If a matching user is found, the request is processed and the appropriate page is returned to the browser. Otherwise, Web Center displays its login page and prompts the client to log in.

Security

An unauthorized client is unable to send a valid logon ticket because the logon ticket must be validated against the certificate of the ticket-issuing system.

Single sign-on with SAP logon tickets works only for user names up to 12 characters.

The URL to start NetWeaver must include the fully-qualified host name, for example http://myHost.myDomain.com:53000/irj/portal.

1.1.5. Configuring Heap Size

Productive operation of Web Center requires Tomcat to be configured so that it uses a heap of sufficient size, at least 256 MB.

For example, to set initial and maximum heap size to 256MB for Tomcat 8.5 on Windows platforms:

- Activate the Tomcat Configuration Menu (Start → Programs → Apache Tomcat 8.5 → Configure Tomcat). If you have installed Tomcat without start menu entries, run the file TOMCAT_HOME**/bin/tomcat8w.exe**.
- Click the **Java** tab.
- Enter **256** into the **Initial Memory Pool** and **Maximum Memory Pool**.

To do the equivalent setting for UNIX platforms, your environment for starting Tomcat must be set so that JAVA_OPTS includes the related Java Virtual Machine options. Here is an example:

```
JAVA_OPTS="-Xms256M -Xmx256M"
export JAVA_OPTS
```

1.1.6. Setting the Default Language

Web Center supports by default German and English.The default language of your Web Center session depends on your preferred language setting as defined in your browser.The default language is German if the browser's preferred language is set to German; otherwise, it is English.

Setting the preferred language is browser-dependent:

- In **Edge**, open the Settings and more menu and select Settings.In the Languages section, move your preferred language to the top (if not available, click **Add languages** and select it).
- In **Firefox**, open the Applications menu and select Settings.In the Language section, click Set Alternatives... and move your preferred language to the top.(If not yet added, select it from the list of available languages and add it.)
- In **Chrome**, select the Customize and control Google Chrome menu and open Settings.In the Advanced/Languages section, move your preferred language to the top.(If not yet added, select it from the list of available languages and add it.)

1.2. About the Web Center Page Layout

Web Center is presented in a default layout that is highly customizable.For details about customizing the page layout, refer to the *DirX Identity Web Center Customization Guide*.The remainder of this section describes the default layout for Web Center.

1.2.1. Default Page Layout

The following figure illustrates the default page layout.Note that because Nik Taspatch has logged in and has administrator privileges, all the available information and most of the menus are displayed; since he is not a business administrator, the business object menus are not visible.If you log in as another user with restricted functionality, you may see only a part of the menus.See the *DirX Identity Provisioning Administration Guide* to learn how to manage menu restrictions.

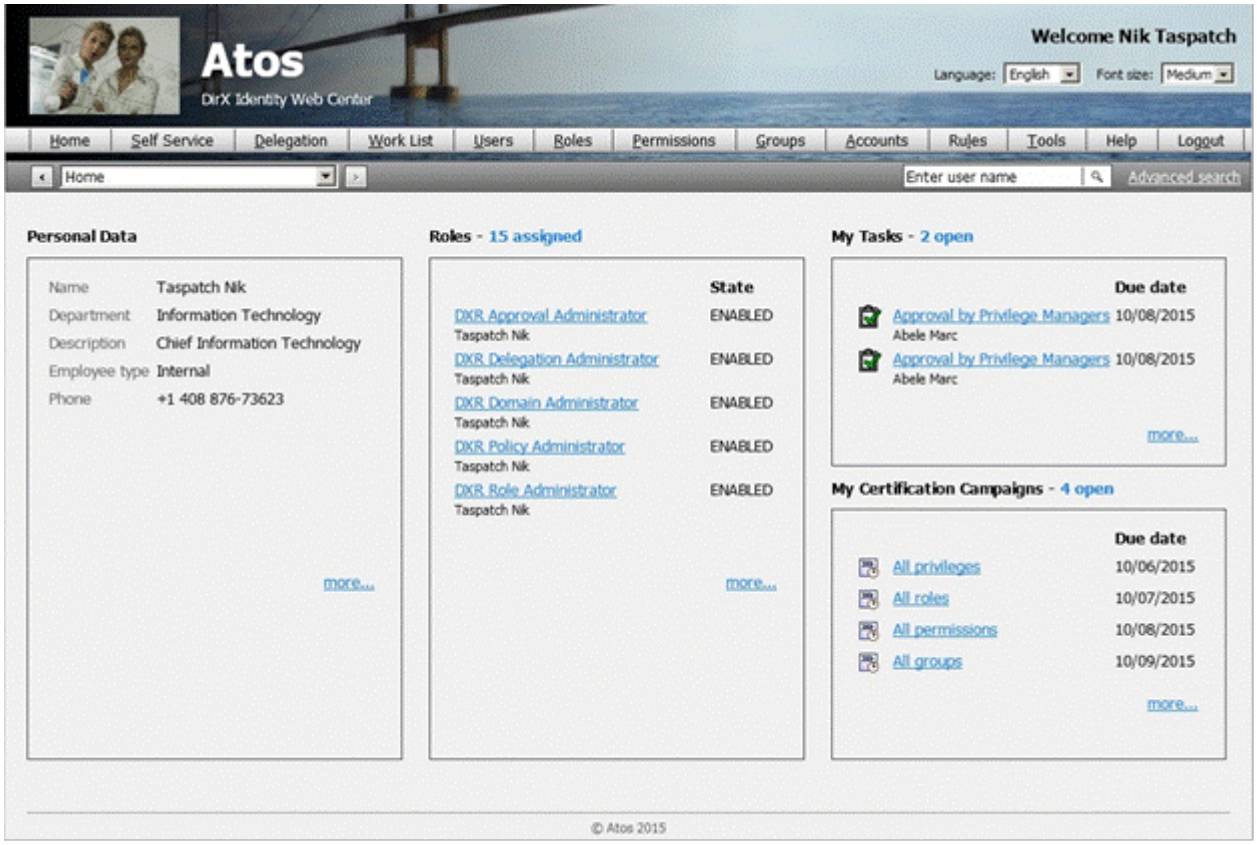

Figure 8. Default Page Layout

The default page layout consists of a header at the top, a menu bar below the header and a footer at the bottom. The rest of the page is application-specific.

All pages contain the same header, which consists of the following items:

A **company logo area** that displays the company's logo and its name.

A **welcome message** that identifies the logged-in user.

A **navigation history chooser** that allows you to return to pages you've previously displayed. Click the down arrow and then choose a page from the list. The browser

redirects to the page with the parameters you previously selected.

A **language chooser** that allows you to display the page in a specific language. Click the down arrow and choose your language. The browser then displays the page in the language you have selected.

A **font size chooser** that allows you to display the page in a specific font size. Click the down arrow and choose the font size. The browser then displays the page in the font size you have selected.

The menu bar displays all menus and operations that the logged-in user is allowed to perform. You can use shortcut keys. In Edge and Chrome, type the ALT + s keys to open the Self Service menu, and then type the c key to perform a password modification; in Firefox, type SHIFT +ALT + s to open the menu. You can browse through the menus with mouse movements and cursor keys (up, left and so on).

The footer of the page displays information like the application version number, copyright information, and installation information. Note that version number and installation information are not visible by default.

The middle of the page is application-specific. The above sample page displays four panels:

- **Personal Data** - displays some of the logged-in user's personal data. Clicking **more ...** in this pane displays detailed personal data provided in the User Summary for the logged-in user. See the section "Display Summary" in "Using the Self Service Menu" for details.
- **Roles** - lists the logged-in user's assigned roles and their state. Clicking **more ...** in this pane opens the **Role** tab in the User Summary for the logged-in user. See the section "Display Summary" in "Using the Self Service Menu" for details.
- **My Tasks** - lists the outstanding tasks (if any) that the logged-in user needs to perform. Clicking **more ...** in this pane displays the task list for the logged-in user. See the section "Task List" in "Using the Work List Menu" for details.
- **My Certification Campaigns** - lists up to five certification campaigns with open tasks for the logged-in user. Clicking **more ...** in this pane leads to the complete list. See the section "Certification Campaign List" in "Using the Work List Menu" for details.

Clicking **Home** in the menu bar displays this part of the default page.

1.2.2. Common Features for All Pages

This section describes common features for all pages:

- How to work with forms.
- How to search and select specific items.
- How to work with item lists.
- How to use special widgets like the calendar widget and tab panels.

1.2.2.1. Working with Forms

Forms are comprised of up to three components:

- The form heading
- The form content
- Form buttons

1.2.2.1.1. About the Form Heading

Form headings appear only on summary pages. They display a form title and a toolbar. The tools in the toolbar perform actions that are applied to the displayed entry:

- The refresh tool  refreshes the summary page.
- The other tools serve as shortcuts for corresponding menu items. For example, the edit tool  opens the page to edit the entry.

The tools in a form toolbar vary with the type of the displayed entry and the access rights of the logged-in user.

Move the mouse over a tool to get a tool tip.

You can navigate to the toolbar with the “tab” key. Then use the keys “left” and “right” to browse through the tools. To select a tool, press “space” or “enter”.

1.2.2.1.2. About Form Content

Web Center displays editable fields with a black border and non-editable fields with a light gray border. Mandatory input fields are indicated by an asterisk following their label. Empty mandatory fields and fields with invalid input are displayed with a pink background.

Use the tab key to navigate through the fields.

In drop-down lists, enter a character to jump to the first list entry starting with this character. Or use the keys “up”, “down”, “home”, “end”, “page up” and “page down” to browse through the list.

Click the  button to search for and select a specific object or item, for example, a workflow or a manager. A page displaying the search panel opens.

1.2.2.1.3. Using the Form Buttons

Web Center forms may include one or more of the following buttons to submit changes to the server or to cancel an operation:

- **Save** to submit and save the modifications.
- **Save and finish** to submit the modifications and then start the operation.
- **Save current state** to submit the modifications without starting the operation.
- **Reset** to discard the modifications.

- **Cancel** to abort the operation.
- **Cancel selection. Back to main page** to abort a select operation and to return to the main page; for example, to return from the page to select a user's manager to the modify user page without selecting a new manager.
- **Do later** to discard any changes and postpone a task.

Clicking one of these buttons locks the form.

1.2.2.1.4. Specifying Due Dates

The form buttons section often includes a field to specify a due date for a create, modify, delete or assignment operation. If you set a due date, the requested operation is not performed immediately. Instead, a ticket with the order to perform the action on the specified date is created. See "Using the Tickets View" in the section "Using the Provisioning Views" in the chapter "Using DirX Identity Manager" for information about tickets.

1.2.2.2. Using the Search Panel

When searching for items, a search panel is displayed to specify the search base and the filter items for the search request. The following figure illustrates the search panel:

Figure 9: Search Panel

The **Search base** field specifies the node in the directory tree at which the search operation starts. Use the tree browser button  to browse to a node in the directory tree - for example, when specifying the search base in the Select User dialog - instead of specifying the user's common name.

The **Search for** row specifies the filter expression for the search request:

- In the first field, click the down arrow to display the list of available search attributes. Select the attribute from the drop-down list. The default attribute is Name (the common name cn).
- In the second field, click the down arrow button to display the available search operators. Select the operator from the drop-down list.
- In the third field, type or select the search filter value. The field varies with the selected attribute and is either a text input field, a date field or a drop-down list.
- Use the  button to display an additional line for specifying a filter-item for the search request; use the  button to delete the last filter-item of the filter-item list; and use the **Search**-button to start the search operation.

The search result is displayed in an item list below the search panel.

If too many items are found, a message is displayed indicating that the size limit has been exceeded. Try to refine your search by specifying additional filter items.

all Web Center menus provide two quick search fields for finding users: the **Enter user name** field, where you can type in the common name in the space provided and an **Advanced Search** button, which takes you to the

user search panel.

1.2.2.3. Working with Item Lists

Item lists are comprised of up to four components:

- The paging bar
- The list heading
- The list headers
- The list items

1.2.2.3.1. Using the Paging Bar

The paging bar displays the index range of the currently displayed items, the total number of items in the list and the number of selected items. Buttons allow you to navigate to the first, the previous, the next and the last page. You can also enter the index of a page in order to directly go to that page. The paging bar is usually displayed on top of each list and repeated below the list. Some lists, however, display the bar only on top or below in order to avoid crammed pages. Item lists that fit on a single page display only the number of selected items.

1.2.2.3.2. Using the List Heading

The list heading displays a toolbar and a page size selector.

The tools in the toolbar perform actions that are applied to all entries in the list:

- The delete button  deletes all the listed items (not available for Users or Accounts). When you click this button, Web Center displays a dialog asking you to confirm the operation.
- The run report button  runs a report on the listed items. See the section "Run Reports" in "Using the Tools Menu" and also the Run Report sections in the Users, Roles, Permissions, Groups, Accounts, Rules and Business Objects menu descriptions in this chapter for a description of this operation.
- The export button  exports the listed items to a file. When you click this button, the browser opens a dialog that allows you to save the list (in HTML format) to a file on your computer. You can then, for example, drag the file onto an open Excel sheet in order to process the data further with Excel.

Some lists display only partial toolbars (usually without the delete tool), while some others do not display a toolbar at all.

Move the mouse over a tool to display a tool tip.

You can navigate to the toolbar with the “tab” key. Then use the keys “left” and “right” to browse through the tools. To select a tool press “space” or “enter”.

The page size selector allows you to control the number of entries displayed on one list page:

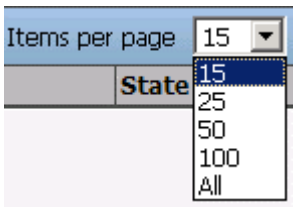

Figure 9. Figure 10: Items per Page Control

1.2.2.3.3. Using List Headers

The list header row displays the column titles, a sort column indicator and some flags.

You can sort the listed entries in any displayed table by most columns. An arrow in the column header indicates the column by which the table entries are currently sorted; a down-arrow indicates a descending sort order, while an up-arrow indicates an ascending sort order.

A small red triangle in the upper left corner of a header indicates that you can modify the data in this column. A small green triangle indicates that you can select a list item by clicking the item's cell in this column.

Some column headers display a checkbox instead of a title. The checkbox allows you to check or uncheck all checkboxes in the column with a single click.

1.2.2.3.4. Using List Items

At many places where objects or links are displayed, you can display the details by clicking the object or link. You can also use the follow-link button ⇒.

To select an item in an item list, check the checkbox at the beginning of the list item row, if one is provided. To select all list items, check the corresponding checkbox in the header row.

Right-click a list item to display a context-sensitive menu, if one is available. The context-sensitive menu provides operations for the following categories:

- **Entry** - provides all operations that can be performed for the highlighted list item. Usually this is a subset of the operations that the entry type specific menu provides, for example **Display Summary**, **Modify Data**, and so on for entry type user. You may not be allowed to perform all displayed operations for all list items.
- **Selected entries** - provides all operations that can be performed for all manually selected list items, for example **Delete** and **Run Report** for entry type location.
- **List** - provides all operations that can be performed on the complete list. (No extra selection is necessary.) Usually these are the operations **Run Report** and **Export**.

See the operation descriptions for details.

1.2.2.4. Using Special Widgets

This section describes how to use special Web Center widgets for specifying dates, browsing and making assignments.

1.2.2.4.1. Specifying Dates

The calendar widget lets you select a date, for example a start date or an end date. Editable form fields of type date display the button to their right. Click the button to open the calendar widget. Editable table cells of type date initially just display the date (if any). To edit the value, click on the cell. The cell content changes to an input field displaying the date, followed by the button. Again, click the button to open the calendar widget.

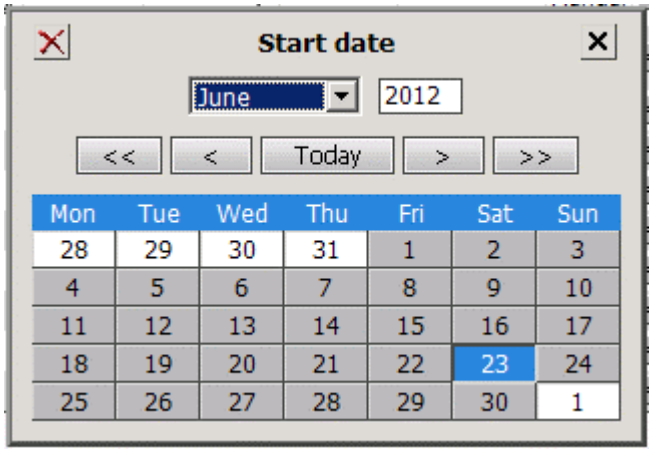

Figure 10. Calendar

The widget contains a button for each day of the selected month and some days of the adjacent months. Click on a day button to select the day. To select the current day, click **Today**.

Use the **<<** and **>>** buttons to switch to the previous and the next year, respectively, or enter a year directly in the corresponding input field. Use the **<** and **>** buttons to switch to the previous and the next month, or select a month from the selection field.

Click to delete the date and close the calendar. Click to close the calendar without changing the date.

You can navigate to each field using the tab key. In the day button panel, you can also move around with the “left”, “right”, “top” and “down” keys. To close the widget, press the escape (Esc) key.

1.2.2.4.2. Specifying Date and Time

A variant of the calendar widget lets you enter the time in addition to the date.

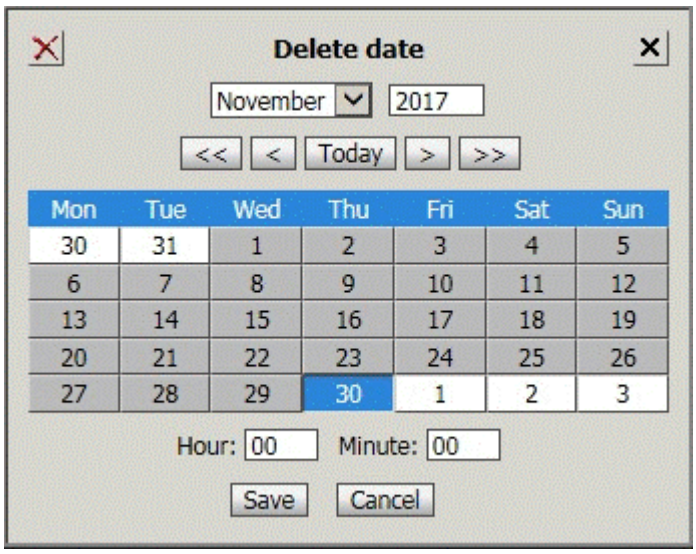

Figure 11. Calendar with Time

The widget includes input fields for hour (0 - 23) and minute (0 - 59). Click **Save** to save your input. Click **Cancel** to close the widget without changing the current date and time.

1.2.2.4.3. Using the Tree Widget

The tree widget allows you to select an entry by navigating to it in the hierarchical object tree. Use the tree, for example, to select the search base in search panels or to select values for role parameters of type hierarchical DN. You open the tree by clicking on the icon.

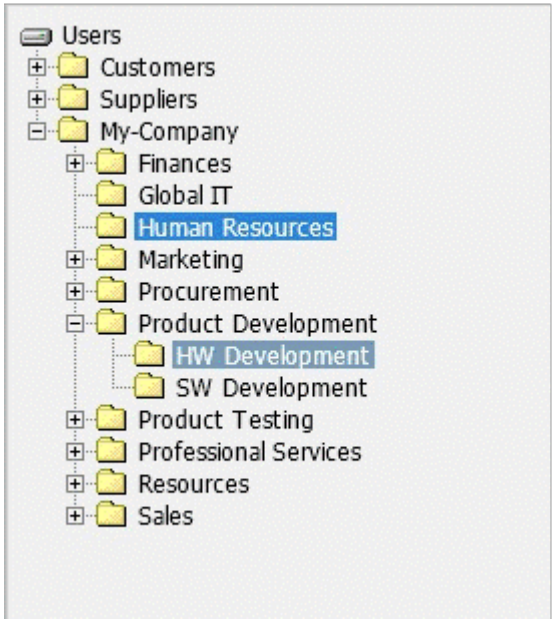

Figure 12. Tree Widget

The tree highlights the currently selected item with a bright blue background. Click the + icon preceding an entry to open an entry; that is, to list its children. Click the − icon to close the subtree below it. To select an entry, just click on it. The tree will close.

The currently focused item is highlighted with a pale blue background. It is used when navigating the tree with keys. You can use the “right” key to open the focused entry and “left” key to close the subtree below it. To move the focus to another item, press “up”,

“down”, “page up”, “page down”, “home” or “end”. To select an entry, press “enter”.

1.2.2.4.4. Using Tab Panels

Some summary pages do not display all available data at once. They show a basic set of properties and one or more tab panels that let you request additional data if needed. For example, the user summary page displays a privilege tab panel to request the user’s assigned roles, permissions, groups and accounts, and another tab panel to get his photo and certificates. Click on a button in the tab panel to load the respective additional information.

Each tab panel is accompanied by an icon bar with some or all of the following icons:

 - displays all tabs one below the other. Downloads each tab not yet downloaded. Does not refresh already downloaded tabs.

 - refreshes all currently visible tabs (except for account groups, when displaying a summary of user data). Does not refresh or download any tab currently not visible.

 - hides the visible tabs or shows the last recently visible tabs.Does not refresh or download any tab.

 - displays all tabs already downloaded one below the other.Does not refresh or download any tab.

1.2.2.4.5. Using the Assignment Widget

Some pages let you assign objects to another object; for example, roles to a user.The assignment widget contains two lists.The upper list of available items shows items that you may assign, while the lower list of assigned items shows the items that are already assigned.The list of available items is accompanied by a search panel that lets you search for items that you want to assign.You can select items in both lists.

The two lists are separated by buttons that specify what to do with the selected items.If two item lists are displayed, use the arrow-down button  to move selected list items from the upper list to the lower list.Use the arrow-up button  to move selected list items from the lower list to the upper list.If available, use the double arrow-down button ⇊ to move all list items from the upper list to the lower list.Use the double arrow-up button ⇈ to move all list items from the lower list to the upper list.Note that the arrow buttons do not save the assignments and unassignments.When finished, click **Save** to persist your changes.

1.3. Logging In to Web Center

Working with the Web Center application is straight-forward and very easy.Open your Internet browser and type the URL for the application:

- **http://***someserver*:_port_**/webCenter-***technicalDomainName*

where

someserver

Specifies the Web server address.

port

Specifies the Web server port number.

technicalDomainName

Specifies the technical domain name that you administered when configuring your system. (See section "Domain Configuration" in chapter "Configuring DirX Identity" in the *DirX Identity Installation Guide* for details.)

Example:

http://localhost:8080/webCenter-My-Company

Tomcat usually uses the port number 8080.

The Web Center next displays the login page, which contains the following fields:

Name - your common name (usually your last name followed by your first name). If configured, you can also specify only a part of the common name.

Password - your password to log in to the directory service.

On this page, you can click:

Log in - to submit the login values in **Name** and **Password** to the server.

If the subsequent search for a DirX Identity user matching the entered name returns a unique user and if his password matches, Web Center accepts the login request.

If the password you supply is incorrect, a page is displayed that allows you to reenter it.

Password Forgotten - to display a dialog with challenge / response questions that allows you to set a new password.

Web Center displays a configurable random selection of the challenge questions you have set up with the Self-Service dialog Add Authentication Questions.If you answer it correctly, you are allowed to change your password.

Register - to use the self-registration dialog to create a login account with Web Center.The register button is shown only if self registration is enabled.

If you are not yet registered, click this button and follow the instructions.

1.4. Logging Out of Web Center

To log out, click **Logout** and then click **Yes** in the dialog box displayed.

1.5. Displaying the Help File

To display the help file, click **Help** in the menu bar.

1.6. Using the Self Service Menu

This section describes how to use Web Center's Self-Service operations, including:

- Display Summary - displays a summary of your data and assignments
- Change Password - changes your password
- Authentication Questions - manages your challenge / response questions and answers
- Modify User Data - changes selected attributes of your user data
- Modify Photos and Certificates - upload or delete your photos and certificates
- Subscribe Privileges - self-assign services
- Show Subscription Status - displays the status of approval workflows running on your behalf
- Show SoD Violations - displays approved and pending segregation of duty (SoD) violations

1.6.1. Display Summary

This operation displays a summary of your user data, including general data, your assigned roles (only if the DirX Identity Provisioning package is installed), permissions, groups and accounts. All the fields displayed in this page are read-only. See the context-sensitive help in the DirX Identity Manager or in the *DirX Identity Connectivity* or *Provisioning Administration Guide* for a description of the fields displayed in this page.

Click **User Facets**, **Personas** or **Functional Users** to display your related user facets, personas or functional users. Click **Roles**, **Permissions**, **Groups**, or **Accounts** to display your assigned privileges and your accounts. Click **Photos** or **Certificates** to display your photos and certificates. When you click one of these buttons, the corresponding tab is displayed, which hides the currently visible tabs. If the tab has already been downloaded, it is re-displayed but not refreshed.

If you have displayed your personas, you can select **Exchange persona and identity** from the context menu to switch the roles of persona and user. If you have displayed your accounts, you can click the  button to display the account's groups.

You can also click one of the shortcut buttons to display this information. (See section "Using Shortcut Buttons" in the section "About the Web Center Page Layout" for details.)

1.6.2. Change Password

Use this operation to change your password. The Password policy section shows the password policies that apply to your entry. When you change your password, the password you choose must comply with these policies. If there is no password policy, this part of the

page is empty.

The Enter password section provides fields for entering the old password and entering a new password twice. Click in the space provided in **Old password** and then enter your old password. Next, click the space provided in **New password** and enter the new password according to the criteria (if any) shown in **Password policy**. Click in **Repeat password** and then enter the new password again.

Click **Save** to start the password change process or click **Cancel** to exit the operation and return to your user summary.

1.6.3. Authentication Questions

Use this operation to manage the authentication (challenge/response) questions to be displayed if you have forgotten your password.

The authentication questions are separated in up to three sections:

- **Mandatory Questions** - Your system administrator may define some questions that must be answered when authenticating via challenge/response. If so, you must define answers for these questions here.
- **Questions from Proposal List** - If your system administrator has defined a list of questions suitable for challenge/response authentications, you can select and answer questions from that list here. Click the down-arrow to open the list.
- **Other Questions** - You can enter and answer any question you like here provided your system administrator has not disabled free text questions.

To add challenge/response pairs to a section, click  at the end of the section. To remove a challenge/response pair, click  in the corresponding row.

Click **Submit** to store your data. Click **Cancel** to return to the user summary without saving your changes.

Notes:

- Answers are case-sensitive. When authenticating via challenge / response later on, you must specify the answers exactly as entered here.
- Questions are always displayed in clear text, while answers are always hidden. On input, you see only the number of characters you entered. Since the answers are stored in hashed format, it is impossible to recover and display them later. However, you can overwrite your answers at any time.
- Your system administrator can define some requirements and restrictions on challenge/response pairs, including:
- The minimum number of questions to define and answer.
- The minimum response length.
- Whether identical answers to different questions are permitted.

1.6.4. Modify User Data

Use this operation to make changes to your user data. Web Center displays many of your user attributes but allows you to edit only those attributes that have been configured to be modifiable.

1.6.5. Modify Photos and Certificates

Use this operation to upload a new photo or a new certificate from a file or to delete existing photos and certificates.

1.6.6. Subscribe Privileges

This operation displays all privileges that you can assign to yourself. The column **Requires Approval** shows whether an approval is necessary to obtain the service. If the field is checked, an approval workflow is started. You can view the status of this workflow with Show subscription status.

Check the boxes of all services to which you want to subscribe and then click **Save**. Use the **Cancel** button to discard the changes and return to the user summary.

1.6.7. Show Subscription Status

Use this operation to display all running, succeeded or failed approval workflows for privilege assignments to you or for modifications of your user data.Click a workflow in the list to display its approval details.(See also the section "Show Initiated Workflows" for details.)

1.6.8. Show SoD Violations

Use this operation to display all pending or approved segregation of duty (SoD) violations.

Approved SoD violations lists the violations that have already been approved. **Pending SoD violations** lists the SoD violations that are still awaiting approval.Click "Show subscription status" to view the status of the approval workflows and to find out who must approve.

1.7. Using the Old Delegation Menu

As of DirX Identity Version 8.9, the delegation feature has been completely redesigned and re-implemented.Web Center supports both the old and the new implementation.This chapter describes the user interface for the old implementation.It is only displayed if the old delegation implementation is enabled.

This section describes how to use Web Center’s older Delegation operations, including:

- Show Access Rights - displays your current access rights and the access rights granted to you by others.
- Delegate Access Rights - delegates the access rights that you are permitted to delegate.

- Show Delegated Access Rights - displays the access rights that you have delegated.

1.7.1. Show Access Rights

Use this operation to display your current access rights and the access rights that others have delegated to you.

Your Current Access Rights provides a summary of all active access rights. The information displayed provides:

- The operation that you are allowed to perform. (See section "Managing Access Policies" in the *DirX Identity Provisioning Administration Guide* for details.)
- The object type for these access rights.
- A description for the access right.

Click an access right or the follow-link button ⇒ to display the access right details.

Access Rights Delegated to You displays the access rights that are currently delegated to you. Delegated access rights can include delegations that are not yet active (the time frame is either in the past or in the future); these access rights are not included in the list. See the context-sensitive help in the DirX Identity Manager or in the *DirX Identity Connectivity* or *Provisioning Administration Guide* for details on the information displayed.

Click a delegation or the follow-link button ⇒ to display the delegation details.

1.7.2. Delegate Access Rights

You can use this operation to delegate your own access rights to other persons.

First, you must select the person to whom you want to delegate your access rights. The operation displays the **Select a User for Delegation** dialog, which allows you to search for and select a user.

Next, the **Modify Delegation** dialog opens. In the upper part of the page, specify the delegation properties. See the context-sensitive help in the DirX Identity Manager or in the *DirX Identity Connectivity* or *Provisioning Administration Guide* for details on the delegation properties displayed.

Below the delegation properties, the list of "Non-granted access rights" is displayed. This list contains all your access rights. You have obtained these rights either from access policies or from delegations by other persons. See the context-sensitive help in the DirX Identity Manager or in the *DirX Identity Connectivity* or *Provisioning Administration Guide* for details on the access right properties displayed.

You can click the follow-link button ⇒ to display the access right details. Here you can modify the access right as necessary.

To delegate access rights:

- Select the access rights you want to delegate. (Check the checkbox of these access

rights.)

- Click the arrow down-button  to move the selected access rights to the "Permanent access rights" list below the "Non-granted access rights" list.
- Click **Save** to save your modifications. The access rights of the "Permanent access rights" list are delegated to the user you selected. The operation displays a message and then opens the "Show delegated access rights" page, which displays a list of all access rights you have delegated.

1.7.3. Show Delegated Access Rights

Use this operation to display all delegated access rights.See the context-sensitive help in the DirX Identity Manager or in the *DirX Identity Connectivity* or *Provisioning Administration Guide* for details on the information displayed.

You can click a row to modify this delegation at any time.You cannot change the user, but you can change any of the other details (for example, you can extend the time period for the delegation because your vacation duration is longer).

When you have finished, click **Save** to save your modified delegation or click **Cancel** to abort the modification process.

You can also select delegations and delete them.Click **Delete Selected Delegations** to perform this task.

1.8. Using the New Delegation Menu

As of DirX Identity Version 8.9, the delegation feature has been completely redesigned and re-implemented.Web Center supports both the old and the new implementation.This section describes the user interface for the new implementation, which is only displayed if the new delegation implementation is enabled.It describes how to use Web Center's new Delegation operations, including:

- **List Delegations** – lists the delegations assigned by you and the delegations assigned to you.
- **Create New Delegation** – creates a new delegation assigned by you.

It also describes how to modify, forward, and delete delegations.

1.8.1. Listing Delegations

Use this operation to display the delegations you have assigned to someone else and the delegations someone else has assigned to you.

Delegations assigned by you provides the list of delegations you have assigned to someone else. The information displayed provides:

- The delegation name and description.
- The operation, either **Assign privileges** or **Approve requests**.

- The name and department of the substitute.
- The delegation start date and end date.

Click an access right or the follow-link button ⇒ to display the access right details.

Delegations assigned to you provides the list of delegations someone else has assigned to you. The information displayed provides:

- The delegation name and description.
- The operation, either **Assign privileges** or **Approve requests**.
- The name and department of the delegator.
- The delegation start date and end date.

Click a delegation or the follow-link button ⇒ to display the delegation details.

1.8.2. Creating New Delegations

Use this operation to delegate your own access rights to other users.

To create a new delegation, enter the name and description of the new delegation and then select the substitute and the operation. Set the start date and end date as appropriate. If the substitute is allowed to forward the new delegation to another user, check **Forwarding permitted**. Finally, click **Save** to save the new delegation.

1.8.3. Modifying Delegations

To modify a delegation, select the menu item **List Delegations**. In the list **Delegations assigned by you**, click the delegation you want to modify. The delegation details page is displayed. Click **Modify delegation** in the toolbar and then change the delegation data as appropriate. You cannot change the substitute.

1.8.4. Forwarding Delegations

To forward a delegation, select the menu item **List Delegations**.In the list **Delegations assigned to you**, click the delegation you want to forward to a new substitute.The delegation details page is displayed.Click **Forward delegation** in the toolbar.Select the new substitute and change the other attributes as appropriate.You cannot change the operation.

Forwarding a delegation creates a new delegation while retaining the original one.

1.8.5. Deleting Delegations

To delete a delegation, select the menu item **List Delegations**.In the list **Delegations assigned by you**, click the delegation you want to delete.The delegation details page is displayed.Click **Delete delegation** in the toolbar and then confirm the deletion.

1.9. Using the Work List Menu

This section describes how to use Web Center's Work List operations, including:

- Task list - shows all tasks that you must execute.
- Certification campaign list - shows certification campaigns with open tasks for you.
- Show initiated workflows - shows all running workflows that you initiated.

1.9.1. Task List

This operation displays all tasks you must handle.For each task in the list, the following properties are provided:

Subject - the workflow display name.

Task - the activity to perform.

For - the object to be handled.

Privilege - the privilege to assign (optional, may be empty).

From - the initiator of the workflow.

Due - the date by which you must complete this task. If you do not complete it in time, the activity will send an email notification to the initiator or escalate this issue.

SoD - whether assigning the privilege would be an SoD violation.

Click one of the tasks in the list to display the details. After completing the task, Web Center displays the details of the next task.

If only one task is pending, the details of this task are displayed (instead of a task list consisting of one item). (See "Task List Details" for more information.)

When displaying the context-sensitive menu select one of the following operations:

Complete one by one - completes the selected tasks one by one.

Change participant - delegates the completion of the selected tasks to another user.

Approve in one step - bulk approval: Approves the selected approval tasks in one step. Tasks not eligible for bulk approval are ignored. A task is eligible for bulk approval if it is an approval task which would not create an SoD violation.

Restrict selection - deselects all tasks that are not eligible for bulk approval.

Select all - selects all tasks that are eligible for bulk approval.

1.9.2. Certification Campaign List

This operation displays the certification campaigns with open tasks for you. For each

campaign, the list displays:

Name - the campaign name.

Due date - the date by which you must complete the certification tasks.

Number of certifications - the number of certification tasks assigned to you.

Owner - the campaign owner.

Description - the campaign description.

Click on a campaign in the list to open its details page. If there's only one campaign with open tasks for you, the operation skips the list and directly opens the campaign's details page.

1.9.2.1. Campaign Details Page

The campaign details page displays:

Name - the campaign name.

Description - the campaign description.

Type - the campaign type, either **User Certification** or **Privilege Certification**.

Owner - the campaign owner.

Due date - the date by which you must complete the certification tasks.

Start date - the date the campaign was started.

1.9.2.1.1. User Certifications

For user certification campaigns, the page also includes:

Users to be certified - the list of users you must certify. The list does not include the users you've already completely certified.

For each user, the list displays:

Name - the user's name.

Department - the user's department.

Phone - the user's phone number.

Due date - the date by which you must complete the subtasks for this user.

Completed - the number of your completed and total subtasks for this user.

Click on a user to open a page that lets you certify the user's privileges.

1.9.2.1.2. Privilege Certifications

For privilege certification campaigns, the page also includes up to three lists:

Roles to be certified - the list of roles you must certify.

Permissions to be certified - the list of permissions you must certify.

Groups to be certified - the list of groups you must certify.

The lists do not include the privileges you've already completely certified. Each list is displayed only if you still have corresponding unfinished certification tasks.

For each privilege, the list displays:

Name - the privilege name.

Folder - the role or permission folder.

Target system - the target system of groups.

Description - the privilege description.

Due date - the date by which you must complete the subtasks for this privilege.

Completed - the number of your completed and total subtasks for this privilege.

Click on an item to open a page that lets you certify the privilege users.

1.9.2.2. Certify User Privileges Page

The page first displays the campaign name and some properties of the user. **Already certified by** lists the approvers that have already certified the user's privileges during the campaign.

The privileges to be certified by you are listed on the **Roles**, **Permissions**, **Groups** tabs and the **Automatically assigned privileges** tab.

To save any changes, click **Save changes**. You can then view and revise your changes later on. If you've taken all your decisions, click **Save changes and finish certification**. This action closes the task; you can no longer view or revise it.

1.9.2.2.1. Roles, Permissions and Groups Tabs

Each tab lists the corresponding privileges to be certified by you. For each privilege, the list displays:

Accept - accept the assignment. To accept all assignments, click the checkbox in the column header.

Reject - reject the assignment. To reject all assignments, click the checkbox in the column header.

Reason - an optional explanation for your decision.

Name - the privilege name.

Folder - the privilege folder (Roles and Permissions tabs only).

Target system - the group's target system (Groups tab only).

Description - the privilege description.

Start date - the assignment's start date. If the start date lies in the future, you can change it. You cannot move it beyond the end date.

End date - the assignment's end date. You can change the end date, but you cannot shift it into the future.

Parameters - the role parameters (Roles tab only). You can remove role parameter values. You cannot remove the last value from a parameter with mandatory value.

Mode - the assignment mode; for example, **Manual**, **BO**, **Rule**.

SoD - whether the assignment constitutes an SoD violation.

When opening a tab, it displays the current certification state of the assignments. The initial certification state on campaign start-up is the state of the actual assignment, with empty **Accept** and **Reject** fields and an empty **Reason** field. The current certification state is the initial state, or the most recent change made by a previous approver or by you. There's no history of changes available.

1.9.2.2.2. Automatically Assigned Privileges Tab

The tab displays the same data as the Roles, Permissions, Groups tabs for privileges automatically assigned to the user; for example, by privilege or business object inheritance, rule or user facets. You can choose to reject an assignment and enter a reason for the rejection. You cannot, however, explicitly accept an assignment or change assignment attributes like start date, end date or role parameters.

Note that rejections of automatically assigned privileges are usually treated differently from rejections of manual assignments at campaign end.

1.9.2.3. Certify Privilege Users Page

The page first displays the campaign name and some properties of the privilege. **Already certified by** lists the approvers that have already certified the privilege users during the campaign.

The list **Users to be certified** displays the users to be certified by you.

Accept - accept the assignment. To accept all assignments, check the box in the column header.

Reject - reject the assignment. To reject all assignments, check the box in the column

header.

Reason - an optional explanation for your decision.

Name - the username.

Risk - the user's risk level.

Department - the user's department.

Phone - the user's telephone number.

Start date - the assignment's start date. If the start date lies in the future, you can change it. You cannot move it beyond the end date.

End date - the assignment's end date. You can change the end date, but you cannot shift it into the future.

Parameters - the role parameters (**Roles** tab only). You can remove role parameter values. You cannot remove the last value from a parameter with a mandatory value.

Mode - the assignment mode; for example, **Manual**, **BO**, **Rule**.

SoD - whether the assignment constitutes an SoD violation.

To save any changes, click **Save changes**.You can then view and revise your changes later.If you've made all your decisions, click **Save changes and finish certification**.This action closes the task; you can no longer view or revise it.

1.9.3. Show Initiated Workflows

This operation displays all subscriptions (running approval workflows) the logged-in user has initiated.(See the section "Workflow List" for details.)

Use the **Succeeded Workflows** button to display all succeeded workflows.Use the **Failed Workflows** button to display all failed workflows.When you click one of these buttons, the corresponding tab is displayed, which hides the currently visible tabs.If the tab has already been downloaded, it is re-displayed but not refreshed.

You can also click one of the shortcut buttons to display this information.(See the section "Using Shortcut Buttons" in the section "About the Web Center Page Layout" for details.)

1.10. Using the Users Menu (User Management)

This section describes how to use Web Center's operations for user management, including:

- Select user - allows you to select a user, user facet, persona, or functional user for a management task.
- Last selection list - displays the result of the last recently performed search query for users.

- Create new user - creates a new user entry.
- Display summary - shows the general data and all assignments of the previously selected user.
- Modify user data - allows you to change the selected user's data.
- Modify photos and certificates - allows you to upload or delete photos and certificates.
- Reset password - allows you to reset the password of the selected user (administrative reset).
- Move user to new destination - changes the folder for the user entry.
- Create new functional user - creates a new functional user for the selected user.
- Create new persona - creates a new persona for the selected user.
- Create new user facet - creates a new user facet for the selected user.
- Assign privileges - allows you to assign privileges to or remove privileges from the selected user.
- Copy privileges - allows you to copy privileges from another user.
- Show subscription status - shows all subscriptions (running approval workflows) for the selected user.
- Task list - shows all tasks of the selected user.
- Certification campaign list - shows the certification campaigns with open tasks for the selected user.
- Show SoD violations - displays all pending or approved segregation of duty (SoD) violations.
- Run report - allows you to run a report on the selected user.

1.10.1. Select User

This operation provides a search utility for user, user facets, persona and functional user entries and displays the list of the entries the search operation returns. The result list contains only the entries you are allowed to view or modify. After you have performed the search, sort the list if necessary and then click one of the entries to work on it.

If user facets, personas and functional users are enabled at the domain level, the search panel includes the check boxes **Include user facets**, **Include personas** and **Include functional users**. Check these boxes to search for user facets, personas and functional users in addition to user entries. Many of the operations for a selected user (like Display Summary and Assign Privileges) also apply to selected user facets, personas and functional users.

For information on how to use the search utility, see the section "Using the Search Panel" in "Common Features for All Pages".

1.10.2. Last Selection List

Use this operation to display the user result list of your most recent search. This page displays the most recently specified search filter.

1.10.3. Create New User

Use this operation to create a new user entry. The process you follow depends on your DirX Identity license (Business or Professional).

1.10.3.1. Professional License:

User creation request workflows define the user creation process. Web Center displays a list of the available user creation workflows that the logged-in user is allowed to run. You must specify the allowed workflows for a user with access policies. If no workflow is available, an error message is displayed.

Select one of the workflows in the list. The sequence of pages displayed next depends on the workflow. When all pages for the logged-in user are completed, the workflow tasks for this user are completed.

1.10.3.2. Business License:

Use this operation to create a new user at a specific location in the directory. If you do not have the access rights to create a new user, an error message is displayed.

This page contains the following fields

Folder - the path where the new user entry is to be created.

The drop-down list allows you to select several possible locations for the new user creation (depending on your access rights). Select the correct root node.

Use the tree browser button to the right of this field to select a specific node under the root node at which to create the new user.

The page displays a set of attributes that can be specified. Enter the necessary values.

Important attributes that you should set (within the sample domain) include:

- All parameters that affect automatic assignment of privileges (policy parameters). In the sample domain, these parameters include EmployeeType, Location, Country.
- The Manager link. It may affect who can change the user later on if the appropriate access policy is set up (as in the sample domain).
- The Password policy to specify special password policies for this user. If you do not specify a password policy, the default policy is used.

After creating the new user, you are automatically forwarded to a page on which to set the initial password for this user: (See the section "Reset Password" for details.)

If necessary, assign or copy privileges.

1.10.4. Display Summary

Use this operation to display a summary of the selected user’s, user facet’s, persona’s or functional user’s data. For details, see the section "Display Summary" in the section "Using

Self Service".

1.10.5. Modify User Data

Use this operation to modify the selected user's data. You can view all the user's attributes, but you can only edit the attributes that have been configured for modification.

1.10.6. Modify Photos and Certificates

Use this operation to upload a new photo or a new certificate from a file or to delete existing photos and certificates.

1.10.7. Reset Password

Use this operation to reset a user's password.

In the Enter password section, enter a new password in the space provided in **New password** according to the password policy (if any) displayed in the Password policy section, or click **Generate** to allow Web Center to create a new password according to the password policy.

Click **Save** to start the reset password operation, or click **Cancel** to exit the operation.

1.10.8. Move User to New Destination

Use this operation to change the folder for the user entry.

1.10.9. Create New Functional User

The Create New Functional User operation is available with the DirX Identity Professional license and is enabled when **Enable Functional User Handling** is checked at the domain.

Like the Create New User operation under the Professional license, the functional user creation process is defined by a creation workflow. The workflow starts with an automatic activity that creates default values (especially for the new functional user's sponsor) for the functional user. All other aspects correspond to the creation of a new user with the Professional license.

1.10.10. Create New Persona

The Create New Persona operation is available with the Professional license and is enabled when **Enable Persona Handling** is checked at the domain.

Like the Create New User operation under the Professional license, the persona creation process is defined by a creation workflow. The workflow starts with an automatic activity that creates default values for the new persona (especially for the new persona's owner) using the selected user as a template. All other aspects correspond to the creation of a new user with the Professional license.

1.10.11. Create New User Facet

The Create New User Facet operation is available with the DirX Identity Professional license and is enabled when **Enable User Facet Handling** is checked at the domain.

Like the Create New User operation under the Professional license, the user facet creation process is defined by a creation workflow. The workflow starts with an automatic activity that creates default values for the new user facet (especially for its owner) using the selected user as a template. All other aspects correspond to the creation of a new user with the Professional license.

1.10.12. Assign Privileges

This page displays the identifying user attributes at the top and below them four tabs for role, permission and group assignments and accounts.

- **Roles** - tab page for assignment modification showing the user's role assignments and a list of all roles that can still be assigned. This tab is only available when the role package is installed.
- **Permissions** - tab page for assignment modification showing the user's permission assignments and a list of all permissions that can still be assigned.
- **Groups** - tab page for assignment modification showing the user's group assignments and a list of all groups that can still be assigned.
- **Accounts** - tab page showing the user's assigned accounts.

Each privilege assignment page provides a search utility for searching for all privileges that you are allowed to assign. See the section "Using the Search Panel" in "Common Features for All Pages" for a description of this utility.

In the upper pane, Web Center displays the privileges that are available for assignment. In the lower pane, Web Center displays all privileges that are already assigned to the user. To select a privilege, click its checkbox and then use the arrow buttons ( or ) to move it between the upper and lower panes. The double-arrow buttons ↓↓ or ↑↑ allow you to move all privileges without having to select them first.

In the Roles tab page, a checked box in the **Parameter** column in the upper pane indicates that this role requires parameters to be specified during assignment. If you select this type of role, Web Center displays additional pop-up pages in which to specify these parameters.

If roles with parameters have been assigned (assigned roles are listed in the lower pane), you can modify the parameter settings at any time by clicking the  button. The page that opens can support a variety of different parameter types. Most types are easy and straightforward to handle. If hierarchical role parameters need to be entered, the control consists of a drop-down list and a tree browser button. Select one of the start nodes from the drop-down list (the start nodes are defined via role parameter access policies). Open the tree browser and navigate to the value you want to assign. Select it. Close the page.

After assignment, the **Parameter** column displays the assigned parameters. If you violate any rules (for example, integer ranges), an error message is visible as a tool tip.

Click **Save** to save your changes. Click **Cancel** to stop the operation and return to the user summary.

1.10.13. Copy Privileges

Use this operation to copy the directly assigned privileges from another user.

This page contains the following fields:

(identification) - identification fields for the selected user (by default, Name, Department and Phone).

(search) - search fields for locating users whose privileges you can copy.

(table) - the users whose privileges you are allowed to copy. Select one of these users.

The next page is identical to the page displayed with the assign privileges operation described in "Assign Privileges". In this case, the page shows the user's original privileges (the privileges that the user had before the copy operation) and the copied privileges, or a warning box that no privileges could be copied, which means that the user whose privileges you copied did not have directly assigned privileges.

You can add or remove privileges and then use **Save** to store the privileges or use **Cancel** to abort the copy operation.

The copy operation works as follows:

- All privilege assignments (roles, permissions, groups) assigned by hand are copied. Privilege assignments with time restrictions (end date, start date) are only copied if the end date is not yet reached.
- Role parameters in assignments are copied.
- Assignments from groups in the IMPORTED state are not copied.
- The privileges are merged: if the user already has a privilege assigned, he is not assigned the same privilege again.
- If a privilege requires approval, an approval workflow is started.

Note: Privileges assigned by rules are not copied because the next execution of the rule would remove or change these rights. Set the permission parameters correctly and run the policy execution service to assign the rest of the privileges via rules.

1.10.14. Show Subscription Status

Use this operation to display the user's subscription status. See the section "Show Subscription Status" in "Using the Self Service Menu" for details.

1.10.15. Task List

This operation displays all tasks of the selected user. See the section "Task List" in "Using the Work List Menu" for details.

1.10.16. Certification Campaign List

This operation displays the certification campaigns with open tasks for the selected user. See the section "Certification Campaign List" in "Using the Work List Menu" for details.

1.10.17. Show SoD Violations

Use this operation to display the user's SoD violations.See the section "Show SoD Violations" in "Using the Self Service Menu" for details.

1.10.18. Run Report

Use this operation to display the reports that you can run on the selected user.The number of reports listed in the page depends on the number of reports configured for this domain and on the access policies that are configured for the logged-in user.If the report list is empty, you are not allowed to run reports on users.

To run a report, click it in the list and then review the displayed result.To download the report to a file, scroll to the bottom of the page and click **Save as file**.Select the correct location and name of the file.

1.11. Using the Roles Menu (Role Management)

This section describes how to use Web Center's operations for role management, including:

- Select Role - selects a role from the list to display its details and manage it.
- Last selection list - displays the result of the last recently performed search query for roles objects.
- Create new role - creates a new role.
- Display summary - displays the summary of the selected role object.
- List users - lists the users the selected role is assigned to.
- Modify role - modifies the selected role object.
- Delete role - deletes the selected role object.
- Assign privileges - assigns or removes privileges (junior roles and permissions) to or from the selected role object.
- Assign users - assigns the selected role to a set of users.
- Remove users - removes the selected role from a set of users.
- Show subscription status - shows all subscriptions (running approval workflows) for the selected role.
- Run report - provides a report about the selected role.

1.11.1. Select Role

This operation provides a search utility for role objects and displays a list of the entries that the search operation returns. The operation displays only the entries you are allowed to

view or modify.

After you have performed the search, sort the list if necessary and then click one of the entries to work on it.

For information on how to use the search utility, see the section "Using the Search Panel" in "Common Features for All Pages".

1.11.2. Last Selection List

Use this operation to display the roles object result list of your most recent search. This page displays the most recently specified search filter.

1.11.3. Create New Role

Use this operation to create a new role at a specific location in the directory. The process you follow depends on your DirX Identity license (Business or Professional).

1.11.3.1. Professional License:

Request workflows define the role creation process. Web Center presents all available workflows that the logged-in user is allowed to run. If no workflow is available, an error message is displayed.

Select one of the displayed workflows in the list. The sequence of pages displayed next depends on the workflow. If there is only one workflow, its pages for specifying input data are displayed.

1.11.3.2. Business License:

If you do not have the access rights to create a new role, an error message is displayed.

This page includes the following fields:

Folder - the path where the new role entry is to be created.

The drop-down list allows you to select several possible locations for the new entry creation (depending on your access rights). Select the correct root node.

Use the tree browser button to the right of this field to select a specific node under the root node at which to create the new role.

The page displays a set of attributes. Enter the necessary values.

After creating the new entry, assign the privileges (junior roles and permissions) to complete the role definition.

1.11.4. Display Summary

Use this operation to display a summary the selected role’s data. The page contains general data, operational attributes, role parameters and the privilege structure. See the context-

sensitive help in the DirX Identity Manager or in the *DirX Identity Connectivity* or *Provisioning Administration Guide* for details on the fields displayed on this page.

All fields are read-only.

1.11.5. List Users

Use this operation to get a list of all users the selected role is assigned to.

1.11.6. Modify Roles

Use this operation to modify the selected role's data. You can view all the attributes, but you can only edit the attributes that have been configured for modification.

1.11.7. Delete Role

Use this operation to delete the selected role.

1.11.8. Assign Privileges

Use this operation to assign privileges to or remove privileges from a role object. This page displays the identifying role attributes at the top and below them two tabs for junior role and permission assignment.

- **Junior Roles** - tab page for assignment modification showing the role's junior role assignments and a list of all roles that can still be assigned.
- **Permissions** - tab page for assignment modification showing the role's permission assignments and a list of all permissions that can still be assigned.

Each privilege assignment page provides a search utility for searching for all privileges that you are allowed to assign. See the section "Using the Search Panel" in "Common Features for All Pages" for a description of this utility.

In the upper pane, Web Center displays the privileges that are available for assignment. In the lower pane, Web Center displays all privileges that are already assigned to the role. To select a privilege, click its checkbox and then use the arrow buttons (or) to move it between the upper and lower panes.

1.11.9. Assign Users

Use this operation to assign the selected role to a set of users. This page displays the identifying role attributes at the top. It provides a search utility to search for user entries in the directory. (See "Select User" in the "Using Users" section for details.) In the search result list, select the users by clicking them or checking the box at the beginning of the list item. Click **Assign** to assign the role to these users.

1.11.10. Remove Users

Use this operation to remove the selected role from users. This page displays the identifying role attributes at the top. It provides a search utility to search for user entries in

the directory with this role. (See "Select User" in the "Using Users" section for details.) In the search result list, select the users by clicking them or checking the box at the beginning of the list item. Click **Remove** to remove the role from these users.

1.11.11. Show Subscription Status

Use this operation to display all subscriptions (running approval workflows) of the selected role.Click one of the list entries to display the approval details.(See the section "Show Initiated Workflows" for details.)

1.11.12. Run Report

Use this operation to display all reports you can run on the selected role.The number of listed reports depends on the number of reports configured for this domain and on the access policies that are configured for the logged-in user.If the report list is empty, you are not allowed to run any report on roles.

To run a report, click it in the list and then review the displayed result.To download the report to a file, scroll to the bottom of the page and click **Save as file**.Select the correct location and name of the file.

1.12. Using the Permissions Menu (Permission Management)

This section describes how to manage permission objects:

- Select permission - selects a permission from the list to display its contents and manage it.
- Last selection list - displays the result of the last recently performed search query for permission objects.
- Create new permission - creates a new permission.
- Display summary - displays the general data and all assignments of the previously selected permission.
- List users - lists the users the selected permission is assigned to.
- Modify permission - modifies the selected permission.
- Delete permission - deletes the selected permission.
- Assign groups - assigns groups to or removes groups from the selected permission.
- Assign users - assigns the selected permission to users.
- Remove users - removes the selected permission from users.
- Show subscription status - shows all subscriptions (running approval workflows) for the selected permission.
- Run report - provides a report about the selected permission.

1.12.1. Select Permission

This operation provides a search utility for permission entries and displays a list of the entries that the search operation returns. The operation displays only the entries you are allowed to view or modify.

After you have performed the search, sort the list if necessary and then click one of the entries to work on it.

For information on how to use the search utility, see the section "Using the Search Panel" in "Common Features for All Pages".

1.12.2. Last Selection List

Use this operation to display the permissions object result list of your most recent search. This page displays the most recently specified search filter.

1.12.3. Create New Permission

Use this operation to create a new permission at a specific location in the directory. Depending on your DirX Identity license (Business or Professional) the operation process is different.

1.12.3.1. Professional License:

Request workflows define the creation of new permissions. Web Center presents all available workflows the logged-in user is allowed to run. If no workflow is available, an error message is displayed.

Select one of the displayed workflows in the list. The sequence of pages displayed next depends on the workflow. If there is only one workflow, its pages for specifying input data are displayed.

1.12.3.2. Business License:

If you do not have the access rights to create a new permission, an error message is displayed.

This page contains the following fields:

Folder - the path where the new permission object entry shall be created.

The drop-down list allows you to select several possible locations for the new entry creation (depending on your access rights). Select the correct root node.

Use the tree browser button to the right of this field to select a specific node under the root node at which to create the new permission.

The page displays a set of attributes. Enter the necessary values.

After creating the new entry, assign the privileges (groups) to complete the permission

definition.

1.12.4. Display Summary

Use this operation to display an overview of the selected permission's data. This page displays general data, approval information, match rules, tasks, and privileges. See the context sensitive help in the DirX Identity Manager or in the *DirX Identity Connectivity* or *Provisioning Administration Guide* for details on the fields displayed.

All fields are read-only.

1.12.5. List Users

Use this operation to get a list of all users the selected permission is assigned to.

1.12.6. Modify Permission

Use this operation to modify the selected permission's data. You can view all the attributes, but you can only edit the attributes that have been configured for modification.

1.12.7. Delete Permission

Use this operation to delete the selected permission.

1.12.8. Assign Groups

Use this operation to assign the selected permission to groups. This page displays the identifying permission attributes at the top and below them a tab for group assignment.

Groups - tab page for assignment modification showing the permission's group assignments and a list of all groups that can still be assigned.

The Groups tab page provides a search utility for searching for all groups that you are allowed to assign. See the section "Using the Search Panel" in "Common Features for All Pages" for a description of this utility.

In the upper pane, Web Center displays the groups available for assignment. In the lower pane, Web Center displays all groups that are already assigned to the permission. To select a group, click its checkbox and then use the arrow buttons ( or ) to move it between the upper and lower panes.

1.12.9. Assign Users

Use this operation to assign the selected permission to a set of users. This page displays the identifying permission attributes at the top. It provides a search utility to search for user entries in the directory. (See "Select User" in the "Using Users" section for details.) In the search result list, select the users by clicking them or checking the box at the beginning of the list item. Click **Assign** to assign the permission to these users.

1.12.10. Remove Users

Use this operation to remove the selected permission from a set of users. This page displays the identifying role attributes at the top. It provides a search utility to search for user entries in the directory with this permission. (See "Select User" in the "Using Users" section for details.) In the search result list, select the users by clicking them or checking the box at the beginning of the list item. Click **Remove** to remove the permission from these users.

1.12.11. Show Subscription Status

Use this operation to display all subscriptions (running approval workflows) of the selected permission.Click one of the list entries to display the approval details.(See also the section "Show Initiated Workflows" for details.)

1.12.12. Run Report

Use this operation to display all reports you can run on the selected permission.The number of listed reports depends on the number of reports configured for this domain and on the access policies that are configured for the logged-in user.If the report list is empty, you are not allowed to run any report on permissions.

To run a report, click it in the list and then review the displayed result.To download the report to a file, scroll to the bottom of the page and click **Save as file**.Select the correct location and name of the file.

1.13. Using the Groups Menu (Group Management)

This section describes how to manage group objects:

- Select group - selects a group from the list to display its contents and manage it.
- Last selection list - displays the result of the last recently performed search query for group objects.
- Create new group - creates a new group.
- Display summary - displays the general data and all assignments of the previously selected group.
- Modify group - modifies the selected group.
- Delete group - deletes the selected group.
- Assign users - adds users to the selected group.
- Remove users - removes users from the selected group.
- Show members - displays the list of members of the selected group.
- Show subscription status - shows all subscriptions (running approval workflows) for the selected group.
- Run report - provides a report about the selected group.

1.13.1. Select Group

This operation provides a search utility for group entries and displays a list of the entries that the search operation returns. The operation displays only the entries you are allowed to view or modify.

After you have performed the search, sort the list if necessary and then click one of the entries to work on it.

For information on how to use the search utility, see the section "Using the Search Panel" in "Common Features for All Pages".

1.13.2. Last Selection List

Use this operation to display the groups object result list of your most recent search. This page displays the most recently specified search filter.

1.13.3. Create New Group

Use this operation to create a new group at a specific location in the directory. Depending on your DirX Identity license (Business or Professional) the operation process is different.

1.13.3.1. Professional License:

Request workflows define the creation of new groups. Web Center presents all available workflows that the logged-in user is allowed to run. If no workflow is available, an error message is displayed.

Select one of the displayed workflows in the list. The sequence of pages displayed next depends on the workflow. If there is only one workflow, its pages for specifying input data are displayed.

1.13.3.2. Business License:

If you do not have the access rights to create a new group, an error message is displayed.

This page includes the following fields:

Folder - the path where the new group object entry is to be created.

The drop-down list allows you to select several possible locations for the new entry creation (depending on your access rights). Select the correct root node.

Use the tree browser button to the right of this field to select a specific node under the root node at which to create the new group.

The page displays a set of attributes. Enter the necessary values.

After creating the new entry, assign the users to complete the group definition.

1.13.4. Display Summary

Use this operation to display an overview of the selected group's data. This page displays general data, approval information, operational attributes, tasks, permission parameters, and privileges. See the context-sensitive help in the DirX Identity Manager or in the *DirX Identity Connectivity* or *Provisioning Administration Guide* for details on the fields displayed on this page.

All fields are read-only.

1.13.5. Modify Group

Use this operation to modify the selected group's data. You can view all the attributes, but you can only edit the attributes that have been configured for modification.

1.13.6. Delete Group

Use this operation to delete the selected group.

1.13.7. Assign Users

Use this operation to add a set of users to the selected group. This page displays the identifying group attributes at the top. It provides a search utility to search for user entries in the directory. (See "Select User" in the "Using Users" section for details.) In the search result list, select the users by clicking them or checking the box at the beginning of the list item. Click **Assign** to add these users to the group.

1.13.8. Remove Users

Use this operation to remove a set of users from the selected group. This page displays the identifying group attributes at the top. It provides a search utility to search for user entries in the directory that are member of this group. (See "Select User" in the "Using Users" section for details.) In the search result list, select the users by clicking them or checking the box at the beginning of the list item. Click **Remove** to remove these users from the group.

1.13.9. Show Members

Use this operation to display all members of the selected group.

1.13.10. Show Subscription Status

Use this operation to display all subscriptions (running approval workflows) of the selected group.Click one of the list entries to display the approval details.(See the section "Show Initiated Workflows" for details.)

1.13.11. Run Report

Use this operation to display all reports you can run on the selected group.The number of listed reports depends on the number of reports configured for this domain and on the

access policies that are configured for the logged-in user.If the report list is empty, you are not allowed to run any report on groups.

To run a report, click it in the list and then review the displayed result.To download the report to a file, scroll to the bottom of the page and click **Save as file**.Select the correct location and name of the file.

1.14. Using the Accounts Menu (Account Management)

This section describes how to use Web Center's operations for account management:

- Select account - allows you to select an account for a management task.
- Last selection list - displays the result of the last recently performed search query for accounts.
- Display summary - shows the general data and all assignments of the previously selected account.
- Modify account - modifies the selected account.
- Display password - displays the password of a privileged account.
- Set password - sets the password of a privileged account.
- Run report - allows you to run a report on the selected account.

1.14.1. Select Account

This operation provides a search utility for account entries and displays the list of the entries the search operation returns. The result list contains only the entries you are allowed to view or modify.

After you have performed the search, sort the list if necessary and then click one of the entries or use the context menu to work on it.

For information on how to use the search utility, see the section "Using the Search Panel" in "Common Features for All Pages".

1.14.2. Last Selection List

Use this operation to display the account result list of your most recent search. This page displays the most recently specified search filter.

1.14.3. Display Summary

Use this operation to display an overview of the selected account's data. This page displays general data, user data, operational data, privileged account data, and groups data. See the context sensitive help in the DirX Identity Manager or in the *DirX Identity Connectivity* or *Provisioning Administration Guide* for details on the fields displayed on this page.

The fields are read-only.

1.14.4. Modify Account

Use this operation to modify the selected account's data. You can view all the attributes, but you can only edit the attributes that have been configured for modification.

1.14.5. Display Password

Use this operation to display the password of a privileged account if you are allowed to read it.

All fields are read-only.

1.14.6. Set Password

Use this operation to set a privileged account's password if you are allowed to perform this operation.

1.14.7. Run Report

Use this operation to display all reports you can run on the selected account.The number of listed reports depends on the number of reports configured for this domain and on the access policies that are configured for the logged-in user.If the report list is empty, you are not allowed to run any report on accounts.

To run a report, click it in the list and then review the displayed result.To download the report to a file, scroll to the bottom of the page and click **Save as file**.Select the correct location and name of the file.

1.15. Using the Rules Menu (Rule Management)

This section describes how to manage rules.It describes how to manage provisioning rules and password policies.

Managing provisioning rules comprises:

- Select rule - selects a provisioning rule from the list to display its contents and manage it.
- Last selection list - displays the result of the last recently performed search query for provisioning rule objects.
- Create new rule - creates a new provisioning rule.
- Display summary - displays the general data and all assignments of the previously selected provisioning rule.
- Modify rule - modifies the selected provisioning rule.
- Delete rule - deletes the selected rule.
- Show subscription status - shows all subscriptions (running approval workflows) for the selected rule.
- Assign privileges - assigns privileges to or removes privileges from the selected

provisioning rule.

- Run report - provides a report about the selected provisioning rule.

Managing password policies

- Manage - manages password policies.

1.15.1. Select Rule

This operation provides a search utility for provisioning rule entries and displays a list of the entries that the search operation returns. The operation displays only the entries you are allowed to view or modify.

After you have performed the search, sort the list if necessary and then click one of the entries to work on it.

For information on how to use the search utility, see the section "Using the Search Panel" in "Common Features for All Pages".

1.15.2. Last Selection List

Use this operation to display the provisioning rule object result list of your most recent search. This page displays the most recently specified search filter.

1.15.3. Create New Rule

Use this operation to create a new rule at a specific location in the directory. The process you follow depends on your DirX Identity license (Business or Professional).

1.15.3.1. Professional License:

Request workflows define the creation of new rules. Web Center presents all available workflows that the logged-in user is allowed to run. If no workflow is available, an error message is displayed.

Select one of the displayed workflows in the list. The sequence of pages displayed next depends on the workflow. If there is only one workflow, its pages for specifying input data are displayed.

1.15.3.2. Business License:

If you do not have the access rights to create a new rule, an error message is displayed.

This page includes the following fields:

Folder - the path where the new rule object entry is to be created.

The drop-down list allows you to select several possible locations for the new entry creation (depending on your access rights). Select the correct root node.

Use the tree browser button to the right of this field to select a specific node under the root

node at which to create the new rule.

The page displays a set of attributes. Enter the necessary values.

After creating the new entry, assign the privileges (roles, permissions, and groups) to complete the rule definition.

1.15.4. Display Summary

Use this operation to display an overview of the selected provisioning rule's data. This page displays general data, operational attributes, more details, role parameters and the privilege structure. See the context-sensitive help in the DirX Identity Manager or in the *DirX Identity Connectivity* or *Provisioning Administration Guide* for details on the fields displayed on this page.

All fields are read-only.

1.15.5. Modify Rule

Use this operation to modify the selected provisioning rule's data. You can view all the attributes, but you can only edit the attributes that have been configured for modification.

1.15.6. Delete Rule

Use this operation to delete the selected rule.

1.15.7. Show Subscription Status

Use this operation to display all subscriptions (running approval workflows) of the selected rule. Click one of the list entries to display the approval details. (See also the section "Show Initiated Workflows" for details.)

1.15.8. Assign Privileges

This operation displays the identifying provisioning rule attributes at the top and below them three tabs for role, permission and group assignments.

- **Roles** - tab page for assignment modification showing the provisioning rule's role assignments and a list of all roles that can still be assigned.
- **Permissions** - tab page for assignment modification showing the provisioning rule's permission assignments and a list of all permissions that can still be assigned.
- **Groups** - tab page for assignment modification showing the provisioning rule's group assignments and a list of all groups that can still be assigned.

Each privilege assignment page provides a search utility for searching for all privileges that you are allowed to assign. See the section "Using the Search Panel" in "Common Features for All Pages" for a description of this utility.

In the upper pane, Web Center displays the privileges that are available for assignment. In

the lower pane, Web Center displays all privileges that are already assigned to the provisioning rule. To select a privilege, click its checkbox and then use the arrow buttons ( or ) to move it between the upper and lower panes.

1.15.9. Run Report

Use this operation to display all reports you can run on the selected provisioning rule. The number of listed reports depends on the number of reports configured for this domain and on the access policies that are configured for the logged-in user. If the report list is empty, you are not allowed to run any report on provisioning rules.

To run a report, click it in the list and then review the displayed result. To download the report to a file, scroll to the bottom of the page and click **Save as file**. Select the correct location and name of the file.

1.15.10. Managing Password Policies

Within this page you can create, modify or delete password policies.A table of existing password policies is displayed at the top.

Creating new password policies - click the Create Password Policy button to create a new password policy.For a description of the password policy parameters see the section "Password Policies" in the *DirX Identity Provisioning Administration Guide* context-sensitive help.

Modifying password policies - click one of the lines in the list of existing password policies to modify it.For a description of the password policy parameters see the section "Password Policies" in the *DirX Identity Provisioning Administration Guide* context-sensitive help.

Deleting password policies - click the checkbox at the end of line of an existing password policy to delete it.You can select several policies.Click the Delete password policies button to remove the selected policies.

1.16. Using the Certifications Menu

This section describes how to use Web Center's operations for certification campaign management, including:

- Select certification campaign - selects a certification campaign from the list to display its details and manage it.
- Create new certification campaign - creates a new certification campaign.
- Display summary - displays the summary of the selected certification campaign object.
- Modify certification campaign - modifies the selected certification campaign object.
- Reset state to "In Preparation" - Resets the state of a certification campaign from “Failed to Start” to “In Preparation”.
- Delete certification campaign - deletes the selected certification campaign object.
- Run report - provides a report about the selected certification campaign.

1.16.1. Select Certification Campaign

This operation displays the list of all certification campaigns you're allowed to view. To view details of a campaign, click the corresponding entry in the list.

1.16.2. Create New Certification Campaign

Use this operation to create a new certification campaign. Define a unique name for the new campaign and assign an owner and then set the optional attributes as required. See the DirX Identity Manager context-sensitive help, the *DirX Identity Connectivity Administration Guide* or the *DirX Identity Provisioning Administration Guide* for a description of the fields on this page.

1.16.3. Display Summary

Use this operation to display a summary of the selected campaign's data. The page contains general data, timing, filter and reminder notification attributes. See the DirX Identity Manager context-sensitive help, the *DirX Identity Connectivity Administration Guide* or the *DirX Identity Provisioning Administration Guide* for a description of the fields on this page.

1.16.4. Modify Certification Campaign

Use this operation to modify the selected certification campaign‘s data. You can view all the attributes, but you can only edit the attributes that have been configured for modification. Once a campaign is running, most of its attributes are read-only.

1.16.5. Reset State to "In Preparation"

If starting a certification campaign fails, its state is set to “Campaign failed to start”. Once you've fixed the problems, use this operation to reset the campaign's state to “Campaign is in preparation” and then adjust the start and due date if necessary. The campaign is then restarted on the scheduled date.

1.16.6. Delete Certification Campaign

Use this operation to delete the selected certification campaign.You can delete only campaigns which are in preparation.

1.16.7. Run Report (Certifications)

Use this operation to display all reports you can run on the selected campaign.The number of listed reports depends on the number of reports configured for this domain and on the access policies that are configured for the logged-in user.If the report list is empty, you are not allowed to run any report on campaigns.

To run a report, click it in the list and then review the displayed result.To download the report to a file, scroll to the bottom of the page and then click **Save as file**.Select the correct location and name of the file.

1.17. Using the Tools Menu

This section describes how to use Web Center's tools:

- **Reports** - run reports on a specific number of selected objects.
- **Upload file** - upload a file to the server.
- **Upload files** - upload one or more files to the server.
- **Upload and process files** - upload one or more files to the server and start a program to process the uploaded files on the server.
- **Show state of uploaded file processing** - display state records that provide information about the progress and outcome of processing uploaded files.

This section describes how to use Web Center's tools:

1.17.1. Reports

Use this operation to run a report on a specific object selection.

This page provides a search utility to specify the objects for the report. In **Objects for the Report**, specify the following search options:

Search base - specifies the search base at which to select the objects for the report. Click the tree browser button  at the end of this field. A pop-up window displays the available object trees. Navigate to the objects you want to select (for example, Role Catalogue).

Scope - specifies the scope of the search. Select one of the following values from the drop-down list:

Subtree search - specifies all objects under this tree node.

One level search - specifies only the next level of objects under this node.

Base DN search - specifies only the node that is the object itself.

Templates lists the available reports for the selected objects. The number of reports displayed here depends on the list of pre-configured reports for this domain and on the access policies for the logged-in user. If the resulting list is empty, you are not allowed to run any report on this object selection.

Click a report in the list to run it. After some time, the report is displayed. To download the report to a file, scroll to the bottom of the page and then click **Save as file**. Select the correct location and name of the file.

1.17.2. Upload File

Use this operation to upload a single file to a specific folder on the server. The file may then be processed on the server by a periodically started background process, by a process watching for changes to the folder, or manually by an administrator.

1.17.3. Upload Files

Use this operation to upload one or more files to a specific folder on the server.The files may then be processed on the server by a periodically started background process, by a process watching for changes to the folder, or manually by an administrator.

1.17.4. Upload and Process File

Use this operation to upload one or more files from the client to the server.For each uploaded file, the server starts a program to process the file.

1.17.5. Show State of Uploaded File Processing

Programs processing uploaded files can write state records giving information about their progress, potential issues and outcome.Use this operation to view the state records of the files you've uploaded.

1.18. Managing Business Objects

Web Center allows administrators to manage the following business objects:

- Countries
- Locations
- Companies
- Departments
- Cost Units
- Contexts
- Projects
- Numbering Plans

Web Center displays the business objects under the common menu line. Click on the business object to display the corresponding menu. You can perform the following operations:

- Select business object - allows you to select a business object.
- Last selection list - displays the result of the last recently performed search query for business objects.
- Create new business object - creates a new business object.
- Display summary - displays the general data and all assignments of the previously selected business object.
- Modify business object - modifies the selected business object.
- Delete business object - deletes the selected business object.
- Show subscription status - shows all subscriptions (running approval workflows) for the selected business object.

- Assign privileges - assigns privileges to or removes privileges from the selected business object
- Run report - provides a report about the selected business object.

The following sections provide information about the operations administrators can perform on business objects.

1.18.1. Select Business Object

This operation provides a search utility for business objects and displays the list of the entries the search operation returns. The result list contains only the entries you are allowed to view or modify.

After you have performed the search, sort the list if necessary and then click one of the entries or use the context menu to work on it.

For information on how to use the search utility, see the section "Using the Search Panel" in "Common Features for All Pages".

1.18.2. Last Selection List

Use this operation to display the business object result list of your most recent search. This page displays the most recently specified search filter.

1.18.3. Create New Business Object

Use this operation to create a new business object at a specific location in the directory. The process you follow depends on your DirX Identity license (Business or Professional).

1.18.3.1. Professional License:

Creating new business objects is defined by request workflows. Web Center presents all of the available workflows that the logged-in user is allowed to run. If no workflow is available, an error message is displayed.

Select one of the displayed workflows in the list. The sequence of pages displayed next depends on the workflow. If there is only one workflow, its pages for specifying input data are displayed.

1.18.3.2. Business License:

Not available.

1.18.4. Display Summary

Use this operation to display an overview of the selected business object's data. This page displays general data, address, operational data, and references. The displayed data depends on the business object type. See the context-sensitive help in the DirX Identity Manager or in the *DirX Identity Connectivity* or *Provisioning Administration Guide* for details on the fields displayed on this page.

All fields are read-only.

1.18.5. Modify Business Object

Use this operation to modify the selected business object's data. You can view all the attributes, but you can only edit the attributes that have been configured for modification.

1.18.6. Delete Business Object

Use this operation to delete the selected business object.

1.18.7. Show Subscription Status

Use this operation to display all subscriptions (running approval workflows) of the selected business object. Click one of the list entries to display the approval details. (See also the section "Show Initiated Workflows" for details.)

1.18.8. Assign Privileges

This operation displays the identifying business object attributes at the top and below them three tabs for role, permission and group assignments.

- **Roles** - tab page for assignment modification showing the business object's role assignments and a list of all roles that can still be assigned.
- **Permissions** - tab page for assignment modification showing the business object's permission assignments and a list of all permissions that can still be assigned.
- **Groups** - tab page for assignment modification showing the business object's group assignments and a list of all groups that can still be assigned.

Each privilege assignment page provides a search utility for searching for all privileges that you are allowed to assign.See the section "Using the Search Panel" in "Common Features for All Pages" for a description of this utility.

In the upper pane, Web Center displays the privileges that are available for assignment.In the lower pane, Web Center displays all privileges that are already assigned to the business object.To select a privilege, click its checkbox and then use the arrow buttons ( or ) to move it between the upper and lower panes.

1.18.9. Run Report

Use this operation to display all reports you can run on the selected business object.The number of listed reports depends on the number of reports configured for this domain and on the access policies that are configured for the logged-in user.If the report list is empty, you are not allowed to run any report on business objects.

To run a report, click it in the list and then review the displayed result.To download the report to a file, scroll to the bottom of the page and click **Save as file**.Select the correct location and name of the file.

1.19. Using the Details Pages

This section explains how to use the Web Center's details pages, including:

- Access rights details
- Delegation details
- Workflow details
- Task list details
- Workflow list

1.19.1. Access Right Details

This page displays the details of an access right. The upper pane provides the following information:

Name - the name of the access right. By default, the name is *Default_**operation* when the access right was calculated from access policies. If it was delegated, the delegator could have changed the name.

Description - an explanation of the access right. The description given by default is **Assembly of all current** *operation* **access rights obtained from access policies or delegations**. If the access right was delegated, the delegator could have changed the description.

Operation - any of the values: approve, grant, modify, read.

Type - the object type for this operation.

The lower pane displays a list of assigned resources. Resources are **Roles**, **Permissions**, **Groups** or **Users**. For each resource in the list, Web Center displays the following information:

Name - the name of the resource.

Type - the type of the resource (role, permission, group or user).

Description - an explanation of the resource.

The user has the right to handle all resources contained in the list with the operation listed in **Operation**.

1.19.2. Delegation Details

Important: the delegation feature provided in the current version of DirX Identity has been completely redesigned and reimplemented. Web Center does not support this new design. The information provided in this section describes the old design, which is supported by Web Center, and applies only if you have not enabled the new implementation.

This page displays the details of a delegation. The upper pane provides the following

information:

Name - the name of the delegation.

Description - an explanation of the delegation.

Delegator - the person who delegated.

Department - the department of the person who delegated.

Start date - (optional) the start date of the delegation.

End date - (optional) the end date of the delegation.

The lower pane displays a list of access rights. For each access right in the list, Web Center provides the following information:

Name - the name of the access right.

Description - an explanation of the access right.

Operation - the operation (approve, grant, modify, read).

Click an access right in the list to display its access right details.

1.19.3. Workflow Details

This page displays the details of a workflow instance. It comprises these fields:

(Type) - the type of workflow. Possible values are:

- Add assignment - the assignment is waiting for approval. After successful approval, the privilege is assigned to the user.
- Modify assignment - the assignment exists already and will be modified. After successful approval, the assignment is modified accordingly.
- Delete assignment - the assignment is to be deleted. After successful approval, the assignment is removed from the user.
- Reapprove assignment - the assignment is waiting for reapproval.
- Create object - an object creation workflow.
- Modify object - a modification approval workflow.
- Delete object - an object deletion workflow.

Subject - the name of the workflow.

Operation - the operation to perform. Possible values are:

- approve - an approval workflow
- create - an object creation workflow
- modify - an object modification workflow

From - the initiator of the workflow.

For - the object the workflow handles.

Start date - the date at which this workflow was started.

End date - the date at which this workflow finished.

State - the status of the workflow. See the section "Understanding Request Workflow States" in the *DirX Identity Provisioning Administration Guide* for more information.

Due - the date at which this workflow expires.

Is expired - an indication that this workflow is already expired.

Running activities - the next lines display the people activities of this workflow that are still running. The available fields in the activity list are:

Activity - the name of the activity.

Participants - the person who has to act.

Start Date - the start date of this activity.

Due - the date when this activity will expire. This causes either another notification dependent on the number of retries or an escalation.

Escalation Level - the current escalation level.

Retry Limit - the number of configured retries.

Finished activities - the next lines display the people activities of this workflow that are still running. The available fields in the activity list are:

End Date - the date when this activity ended.

Activity - the name of the activity.

Participants - the person that performed this activity.

State - the state of the finished activity. See the section "Understanding Request Workflow Activity States" in the *DirX Identity Provisioning Administration Guide* for more information.

Application State - the application state of the finished activity. See the section "Understanding Request Workflow Activity States" in the *DirX Identity Provisioning Administration Guide* for more information.

Reason - the entered reason of the participant.

Cancel workflow - click this button to cancel this workflow. If you are not allowed do cancel this workflow (this is dependent on the configured access policies).

1.19.4. Task List Details

This page displays the details of a task list entry. Its layout is different depending on the task type, but the following fields are common to all pages:

From - the initiator of the workflow. For a user self-registration, this field displays ANYONE.

Due - the due date of this request. It defines further action of workflow engine (either additional notifications or an escalation).

Folder - the location in the directory tree at which this object will be created after approval.

Reason - the reason for this approval. Providing a reason is good practice, especially if you reject the request. This field is not displayed during the confirmation step of a self-registration.

The actions on an approval page are:

- The approver can change some of the values on this page before clicking **Accept**. This feature streamlines approval workflows because it is not necessary to reject the request to inform the initiating user and to wait for the corrected approval request. Note that the administrator can prohibit changing values in the domain configuration or in the workflow configuration. (See "Domain Properties" and "Activity - Activity" in the *DirX Identity Provisioning Administration Guide* for details.)
- **Accept** - click this button to accept this approval request.
- **Reject** - click this button to reject this approval request.

The next sections list specific fields for the different task list types.

1.19.4.1. Approval of Object Creation

The additional fields on this page depend on the specific object type and the workflow definition.

1.19.4.2. Approval of Attribute Modifications

Name - the user entry to be changed.

The next lines display the fields to be modified. The old and new values are listed. The approver can change the new value if it is incorrect.

1.19.4.3. Approval of a Privilege Assignment

The bold title under the **From** field defines the type of approval request for this privilege assignment. Available types are:

- **Add assignment** - the assignment is waiting for approval. After successful approval, the privilege is assigned to the user.
- **Modify assignment** - the assignment exists already and will be modified. After successful approval, the assignment is modified accordingly.

- **Delete assignment** - the assignment is to be deleted. After successful approval, the assignment is removed from the user.

The next fields are:

Folder - the location in the directory tree at which this object will be created or is located.

For - the user to whom the privilege is assigned.

Privilege - the privilege that is assigned.

The next fields list the privilege parameters. For a modification, the new and the old values are displayed. The approver can change the new value if it is incorrect.

SoD violations - a list of segregation of duty violations the approver must take into account.

1.19.5. Workflow List

This page shows a list of workflows. The following fields are displayed:

(selection box) - click this box to select the workflow.

Subject - the display name of the workflow.

Operation - the operation to perform, for example:

- Add assignment - an approval workflow
- Create object - an object creation workflow
- Modify object - an object modification workflow

For - the object the workflow handles.

Privilege - the privilege that is assigned. This field may be empty.

From - the initiator of the workflow.

State - the status of the workflow.

Click one of the displayed lines to see the workflow details.

Click **Cancel selected workflows** to cancel the marked workflows.

2. Using DirX Identity Web Center for Password Management

Identity **Web Center for Password Management** is a web application that provides password change functionality for end users and service desk members. The application runs on Apache Tomcat and can be accessed by standard Internet browsers.

Web Center for Password Management is only available with the password management license. Its configuration and functions overlap with the full Web Center application described in the chapter "Using DirX Identity Web Center".

This chapter describes the features and functions that are specific to Web Center for Password Management and references "Using DirX Identity Web Center" for information about features that are common to both versions.

2.1. Configuring Web Center for Password Management

Configuring Web Center for Password Management consists of the following tasks:

- Using the Web Center configuration file **web.xml**
- Configuring Web Center bind passwords
- Configuring single sign-on
- Configuring heap size
- Setting the default language

All of these tasks are common to both Web Center and Web Center for Password Management and are described in "Configuring Web Center".There are additional configuration parameters that are specific to Web Center for Password Management.For details, see the use case document "Password Management".

2.2. Logging In to Web Center for Password Management

Working with Web Center for Password Management is straight-forward and very easy.Open your Internet browser and type the URL for the application:

- **http://***someserver*:_port_**/pwdManagement-***technicalDomainName*

where

someserver
: Specifies the Web server address.

port

Specifies the Web server port number.

technicalDomainName

Specifies the technical domain name that you administered when configuring your system. (See the section "Domain Configuration" in the chapter "Configuring DirX Identity" in the *DirX Identity Installation Guide* for details.)

Example:

http://localhost:8080/pwdManagement-My-Company

Tomcat usually uses the port number 8080.

Web Center for Password Management next displays the login page, which contains the following fields:

Authentication Domain – your master target system. Click the down arrow to select a target system from the list. This field is only visible when external authentication is enabled and when the Web Center for Password Management's login page is configured to display it. See the use case document "Password Management" for details

Name - your common name (usually your last name followed by your first name) or another kind of login string, for example, the UID or e-mail address, depending on the configuration of Web Center for Password Management. If configured, you can also specify only a part of the common name. In case you selected an authentication domain, your login name in the master target system (can be configured at the target system).

Password - your DirX Identity user password and/or your password in the selected authentication domain.

On this page, you can click:

Log in - to submit the login values in **Name** and **Password** to the server.

Web Center for Password Management compares the number of characters entered in the **Name** field with the value supplied in the **loginForm.minChars** parameter in the **webCenter.properties** file. If the subsequent search returns a unique result, Web Center for Password Management accepts the login request.

If you enter the wrong password you are prompted to correct it.

If you exceed the permitted number of failed logins (which is configured at the domain), your login is locked for some period of time, and you are redirected to the Authentication Questions dialog.

Password Forgotten - to display a dialog with challenge / response questions that allows you to set a new password.

Web Center for Password Management displays a configurable random selection of the challenge questions you have set up with the Self-Service dialog Add Authentication

Questions.If you answer them correctly, you are allowed to change your password.

If you exceed the permitted number of failed attempts to answer authentication questions (which is configured at the domain), you are locked from further attempts for some time.

If you have not supplied your challenge/response questions, Web Center for Password Management prompts you to supply them after successful login.If you choose not to specify them at this time, Web Center for Password Management will prompt you again at your next session.

When you log in successfully to Web Center for Password Management using external authentication and your DirX Identity user password is different from the external master system password, Web Center for Password Management updates the user password with the master target system password and displays an informational message about the password change event.This password update can fail; for example, if the user password policy is inconsistent with the master target system password.

2.3. About the Web Center for Password Management Layout

The Web Center for Password Management page layout is the same as the full Web Center application.See the section "About the Page Layout" in the chapter "Using DirX Identity Web Center" for details.

2.4. Logging Out of Web Center for Password Management

To log out, click **Logout** and then click **Yes** in the dialog box displayed.

2.5. Using the Password Self Service Menu

This section describes how to use Web Center for Password Management Self-Service operations, including:

- Display Summary - displays a summary of your data and the accounts you have in DirX Identity target systems
- Change Password - changes the password of one or more of your accounts
- Authentication Questions - manages your challenge / response questions and answers

2.5.1. Display Summary (Password Management)

This operation displays a summary of your user data, including general data and a list of your accounts in DirX Identity target systems.All the fields displayed in this page are read-only.See the context-sensitive help in the DirX Identity Manager or in the *DirX Identity Connectivity* or *Provisioning Administration Guide* for a description of the fields displayed in this page.

The Accounts section provides information about each account you have in a target system, including the target system name, the account state and the time and result of the last password change. Only accounts suitable for password synchronization are displayed.

2.5.2. Change Password (Password Management)

Use this operation to change your password. You can change your DirX Identity user password, the password of your master account and the passwords of your other accounts. The old password is always the most recent DirX Identity user password. The new password will be applied to the selected entries (User and master account, Other accounts).

The Password policy section shows the password policies that apply to your entry. When you change your password, the password you choose must comply with these policies. If there is no password policy, this part of the page is empty.

The User and master account section provides the **Synchronize password** box. If you want to change the master target system password and the user password, check this box. If you use external authentication the master account is displayed. For initial password setting you cannot uncheck user and master password synchronization

The Other accounts section lists the accounts you have in the connected target systems. To select the accounts whose passwords you want to change, check the box in the **Synchronize Password** column for the account. By default, either all of your accounts are selected (if you have never used this operation before) or the accounts you selected last time you ran the operation are selected.

The Enter password section provides fields for entering the old password and entering a new password twice. Click in the space provided in **Old password** and then enter your old password. Next, click the space provided in **New password** and enter the new password according to the criteria (if any) shown in **Password policy**. Click in **Repeat password** and then enter the new password again.

Click **Submit** to start the password change process, or click **Cancel** to exit the dialog and return to your user summary page.

When you click **Submit**, Web Center for Password Management opens a new page that displays the password change states (pending, succeeded or failed) for the accounts you have selected. The page is automatically refreshed until no more password change is in state pending. To avoid infinite loops, the number of attempts to determine the password changes states is limited.

2.5.3. Authentication Questions (Password Management)

Use this operation to manage the authentication (challenge / response) questions to be displayed if you have forgotten your password.

The authentication questions are separated in up to three sections:

- **Mandatory Questions** - Your system administrator may define some questions that must be answered when authenticating via challenge/response. If so, you must define answers for these questions here.

- **Questions from Proposal List** - If your system administrator has defined a list of questions suitable for challenge/response authentications, you can select and answer questions from that list here. Click the down-arrow to open the list.
- **Other Questions** - You can enter and answer any question you like here provided that your system administrator has not disabled free text questions.

To add a challenge / response pair to a section, select the add icon  at the end of the section. To remove a challenge / response pair, click the delete icon  in the respective row.

Click **Submit** to store your data. Click **Cancel** to return to the user summary without saving your changes.

Notes:

- Answers are case-sensitive.When authenticating via challenge / response later on, you must specify the answers exactly as entered here.
- Questions are always displayed in clear text, answers are always hidden.On input, you see only the number of characters you entered.Since the answers are stored in hashed format, it is impossible to recover and display them later on.However, you can overwrite your answers at any time.
- Your system administrator can define some requirements and restrictions on challenge/response pairs, including:
- The minimum number of questions to define and answer.
- The minimum response length.
- Whether identical answers to different questions are permitted.

2.6. Using the Password Service Desk Menu

This section describes how to use Web Center for Password Management's Service Desk operations, including:

- Users - manages users.
- Password Policies - manages password policies.
- Reports - generates reports on selected password management-related information.

2.6.1. Managing Users

Resetting a user's password from the Web Center for Password Management Service Desk consists of the following steps:

- Selecting the target user
- Viewing user data
- Resetting a user's password
- Releasing locks

The next sections describe these steps.

2.6.1.1. Selecting a User

To select a user, click **Users** and then choose **Select User**. Web Center displays a search panel that allows you to specify the filter items and search base for the request. Use this panel to find and select the user entry that interests you. The search base tree browser lets you select a node in the Users tree from which to start the search. Then use the Search for fields to filter the search, for example, to select only those users whose surnames begin with "F". For details on how to use the search panel, see the section "Using the Search Panel" in "Common Features for All Pages" in "About the Web Center Page Layout" in the chapter "Using Web Center". Start the search by clicking on the Search button.

A simple alternative way to search for users provides the quicksearch control in the navigation bar below the menu.

The search result list is displayed below the search panel. Click on a user to select him and view his summary page or right-click on a user to display the context menu.

2.6.1.2. Viewing User Data

The user summary page displays some user properties, the relevant user accounts with their password change states, and the attributes related to locking login or other authentication attempts (via challenge/response or one-time password). You can, for example, see whether and until when login attempts are locked, the time of the last failed login and the current number of failed logins.

The page's toolbar contains among others icons to refresh the data, to reset the password and to unlock the user.

2.6.1.3. Resetting a User's Password

To reset a user's password,

- Select **Reset password** from the user's context menu in the user list.
- Or click on the **Reset password** icon in the toolbar of the user's summary page.
- Or select the **Reset password** item in the **Users** menu.

2.6.1.3.1. Authenticating the User's Identity

Web Center for Password Management displays the Authenticate Selected User dialog, which allows you to verify the user's identity. The dialog displays the user's name and some of his or her attributes, along with the authentication questions (if any) the user has prepared (see "Authentication Questions" for details).

You can use this information to identify the user; for example, by asking the user for the values of some of the displayed attributes (for example, the user's office telephone number) or asking the user for the answers to some or all of the authentication questions.

If you are using the authentication questions, enter the answers that the user gives into the

Answers field and then click **Verify**. Incorrect or missing answers are highlighted. When you are certain that you have identified the user, click **Confirm**; otherwise, click **Cancel** or continue asking the user.

2.6.1.3.2. Completing the Password Reset

To complete the password reset, click **Confirm**. This action opens the Reset the User's Password dialog.

In the User and master account section, check or clear the **Synchronize password** box.

In the Other accounts section, check or clear the **Synchronize Password** boxes for the user's accounts in the target systems to select or deselect them for password reset.

In the Enter password section, enter a new password in the space provided in **New password** according to the password policy (if any) displayed in the Password policy section, or click **Generate** to allow Web Center to create a new password according to the password policy. Click **Submit** to start the password reset process, or click **Cancel** to abort it. Note that if you cancel, you will still not know the current password.

When you click **Submit**, Web Center for Password Management opens a new page that displays the password change status (pending, succeeded or failed) for the user's accounts you selected. The page is automatically refreshed until no more password change is in state pending.

2.6.1.4. Releasing Locks

To release a user's locks,

- Select **Release locks** from the user's context menu in the user list.
- Or click on the **Release locks** icon in the toolbar of the user's summary page.
- Or select the **Release locks** item in the **Users** menu.

A confirmation box pops up. Confirm that you really want to release the locks.

When confirmed, both locks are released. All lock related attributes are reset. The lock related fields on the user summary page should now be empty.

2.6.2. Managing Password Policies (Password Management)

Use the Password Policies page to create, modify and delete password policies. The top of the page displays a table of existing password policies.

To create a new password policy, click the Create Password Policy button. For a description of the password policy parameters, see the section "Password Policies" in the *DirX Identity Provisioning Administration Guide* and the topic "Password Policy Parameters" in the context-sensitive help.

To change an existing password policy, click it in the list. For a description of the password policy parameters, see the section "Password Policies" in the *DirX Identity Provisioning Administration Guide* and the topic "Password Policy Parameters" in the context-sensitive

help.

To delete an existing password policy, check the box that appears at the beginning of its line. You can select several policies to be deleted. Click the Delete password policies button to remove the selected policies.

2.6.3. Running Reports

The Reports operation allows you to generate reports on selected DirX Identity objects, like users, assignments, privileges, and so on.

To select the objects on which to report, use the **Search base** and **Scope** fields in the Objects for the Report section. In the Templates section, Web Center displays the reports that you can run on the objects you selected.

For example, suppose you want to access the reports you can run on the users in the Finances organizational unit in the My-Company sample domain's Users tree:

- In **Search base**, click the tree browser icon  . In the tree browser pop-up window, navigate to the **Finances** node under **Users** → **My-Company** and then select it. The tree browser window closes and the **Search base** field shows **Finances**, **My-Company**, **Users**.
- In **Scope**, use the drop-down arrow to select the search scope for the selected search base:
- **Subtree search** - searches all objects under the selected tree node.
- **One level search** - searches only the next level of objects under this node.
- **Base DN search** - searches only the selected tree node.
- Now the Templates section lists the available reports you can run on your selected objects. Note the pre-configured reports in the list that relate to Password Management. They are:
- **Number of registered users for Password Management** - generates a report on the number of registered users in each organizational unit (a registered user is a user who has set up authentication questions for password reset; see the section "Authentication Questions" for details).
- **Users with Password Management** - generates a report on users with accounts and attributes related to password management. This report is like the normal user report except for the section on Target System accounts, which shows all the accounts of the user with the target system name, the common name of the account, its state in the connected system, the time and result of the last password change and the normal flags that to indicate that the password cannot be changed, never expires or is not required.
- **Users with password management history** - generates a report on per-user password changes; one password change per line.

The reports displayed in Templates depend on the list of pre-configured reports that the DirX Identity domain provides for the selected objects and on the access policies for the logged-in user. If no report templates are displayed, it means that you are not allowed to run any report on your object selection.

To run a report, click it in the list and then review the displayed result (sometimes it takes a little time for the report to be displayed). To download the report to a file, scroll to the bottom of the page and then click **Save as file**. Select the correct location and name of the file.

3. Using DirX Identity Manager

The topics in this chapter describe DirX Identity Manager features and usage for the Provisioning, Connectivity and Data View groups, including information about:

- Logging in
- Using the main window
- Supplying date and time
- Managing your configuration database
- Handling erroneous field content
- Using wizards
- Using the Provisioning views
- Using the Connectivity views
- Using the Data View
- Customizing DirX Identity Manager

3.1. Logging In

To start DirX Identity Manager:

1. Click **Start**, and then point to **Programs**.
2. Point to **Atos DirX Identity V*x.x*, and then click *Manager**.

Manager displays a splash screen that shows its name and the version.After the splash screen disappears, it displays a view group dialog, as shown in the following figure:

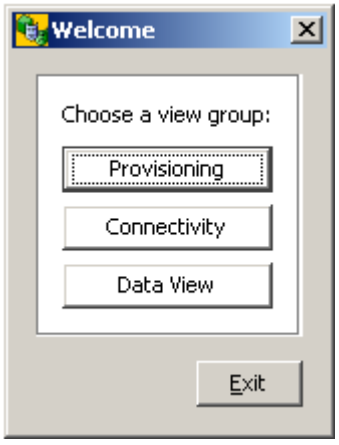

Figure 13. DirX Identity Manager View Group Dialog

Here you can select one of the available view groups. Next, the login dialog is displayed:

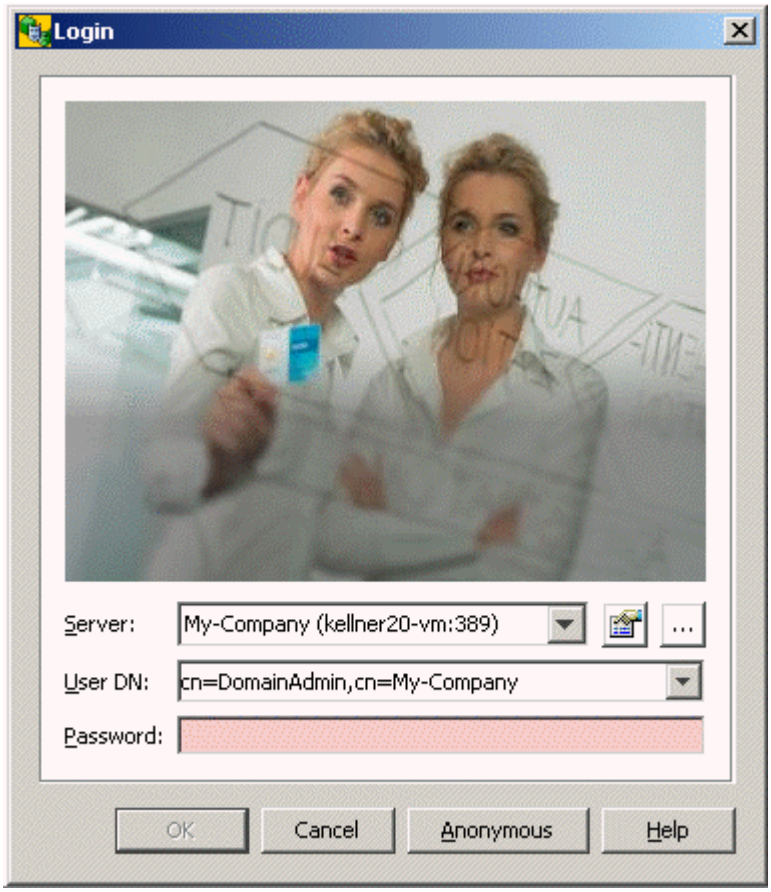

Figure 14. DirX Identity Manager Login Dialog

To log in to Manager:

3. Enter your login profile in **User DN**.Alternatively, you can use the default login profile that Manager has selected for you, if this is your login profile.
4. Enter your password.
5. Click **OK** or press **Enter**.

Manager attempts to log in to the Identity store shown in the **Server** field of the login dialog.If the login operation is successful, Manager closes the login dialog and displays its main window with the previously selected view group.If the login operation fails, Manager displays an error message and places the cursor in the password field.

Read the Login section in the Standard Dialogs chapter in the *Basic Patterns* help module to learn more about the capabilities of the Login dialog.

You can click **Cancel** to cancel the login procedure.Manager closes the login dialog and opens an empty main window.You must restart DirX Identity Manager to log in again.

3.2. Using the Main Window

The main window is a frame around the different views.It consists of window header, a menu bar, a toolbar, a views bar for the selection of a particular view, a work area (divided into several panes whose appearance depends on the selected view) and a status bar.

3.2.1. Using Manager Views

DirX Identity Manager provides the following view groups displayed in the View Bar on the left-hand side of the main window:

- **Connectivity** - shows the DirX Identity Connectivity views: Global View, Expert View, Status Reports view and Monitor View.
- **Provisioning** - shows the DirX Identity Provisioning views: Users, Business Objects, Privileges, Policies, Certification Campaigns, Workflows, Target Systems, Auditing, and Domain Configuration.
- **Data View** - shows the Connectivity data view and Provisioning data view at the LDAP level.

Each different view is composed of a tree or list control and a work area that contains either:

- A map that displays icons that represent connected directories and lines that represent synchronization workflows.
- A property dialog that corresponds to the item that is currently selected in the tree control.

Note: If you need to work with the same view or with different views in parallel, you can start the DirX Identity Manager several times (make sure you have enough main memory to avoid swapping operations). Now you can use the operating system to switch between these views. You can work in all views in parallel. DirX Identity Manager is designed to have the correct information (for correct display you may need to click the Refresh button).

3.2.2. Using the Main Window Menu

The DirX Identity Manager's main window provides the following menu selections:

- File
- Edit
- View
- Tools
- Help

Note that these menu selections are completely disabled when an object is edited in the Connectivity Expert View.

3.2.2.1. File

The File menu contains items that act on a particular configuration object as a whole. The menu selections are:

- **Import** - imports files (only available in the Data View and the Provisioning view)
- **Export** - exports files (only available in the Data View and the Provisioning view)

- **Import Nationalization Items** - imports nationalization item files. See the *DirX Identity Provisioning Administration Guide* for more information about nationalization items.
- **Export Nationalization Items** - exports all nationalization items to a nationalization file. See the *DirX Identity Provisioning Administration Guide* for more information about nationalization items.
- **Properties** - displays the properties of an object. For the connected directory icons and workflow lines in the Global View, this selection opens the configuration wizard. For the Expert View, this selection displays the properties of a selected configuration object in the work area.
- **Exit** - unbinds and closes Manager.

3.2.2.2. Edit

The Edit menu contains all commands to manipulate a particular item. The visibility of the commands depends on the current context.

- **Cut** - standard cut operation (not used in DirX Identity Manager).
- **Copy** - standard copy operation (not used in DirX Identity Manager).
- **Paste** - standard paste operation (not used in DirX Identity Manager).
- **Delete** - standard delete operation. Enabled only when a connected directory icon or workflow line is selected in the Global View or when a configuration object is selected in the tree pane or in the object table (upper right) of the Expert View.
- **Rename** - changes the displayed name of an object. Enabled only when a connected directory icon or workflow line is selected in the Global View or when a configuration object is selected in the tree pane or in the object table (upper right) of the Expert View.

3.2.2.3. View

The view menu contains menu selections that optionally display or hide parts of the main window. The menu selections are:

- **Views Bar** - shows or hides the Views bar, which is the left-most pane. The Views bar contains buttons to select a Manager view.
- **Views → Connectivity → Global View**, **Expert View**, **Status Reports**, **Monitor View** - click to show the corresponding Manager view (this selection is especially useful when the Views bar is hidden).
- **Views → Provisioning → Users**, **Business Objects**, **Privileges**, **Policies**, **Certification Campaigns**, **Workflows**, **Target Systems**, **Auditing**, **Domain Configuration -** click to show the corresponding Manager view (this selection is especially useful when the Views bar is hidden).
- **Views → Data View → Connectivity, Provisioning -** click to show the corresponding Manager view (this selection is especially useful when the Views bar is hidden).
- **Tool Tips** - enables or disables the tool tips.
- **Refresh -** click to refresh the current view.

3.2.2.4. Tools

The tools menu contains only one option for key store management. The menu selections are:

- **Options** - allows you to manage Java keystores.

3.2.2.5. Help

The Help menu contains command items to show selected topics of the online documentation. The selections are:

- **Help** - starts the help system and shows the online manual's table of contents.
- **Contextual help** - starts the "What's This?" help system. Click any item in the current view to get help information about the item.
- **About...** - shows a small window with some useful application information (complete application name, build number, license information).

3.2.3. Using the Main Window Toolbar

DirX Identity Manager's main window provides the following toolbar buttons:

-  Available after jumping from one object to another object in a Provisioning, Connectivity or Data View tree pane. Use this button to return to the previously selected object.
-  Available after jumping from one object to another object and back in a Provisioning, Connectivity or Data View tree pane. Use this button to return to the previously selected object.
-  Allows you to stop an LDAP operation that has been running for a long time.
-  Retrieves the DirX Identity data from the directory service.
-  Displays the properties of an object. This button opens the configuration wizard when used in the Connectivity Global View on connected directory icons and workflow lines. This button displays the properties of a selected configuration object in a new window when used in Provisioning views, the Connectivity Expert View and the Data View.
-  Shows or hides the Views bar, which is the left-most pane. The Views bar contains buttons to select a Manager view.
-  Cuts an object to the clipboard. Only used in the Data View.
-  Copies an object to the clipboard. Only used in the Data View.
-  Pastes an object from the clipboard. Only used in the Data View.
-  Deletes an object. Enabled only when a connected directory icon or workflow line is selected in the Global View or when a configuration object is selected in the tree pane or in the object table (upper right) of the Expert View. Also used in the Data View.
-  Click to view forms in design mode. This feature adds checkboxes before each field. The meaning of the checkbox is:

Checked - This field is visible when design mode is switched off.
Unchecked - This field is not visible when design mode is switched off.
Greyed - This field has been defined at a lower level (can only occur in a wizard in the Global View).

After restarting DirX Identity Manager, design mode is switched off (default setting).
For details about this feature, see the section "Using Design Mode" in the *DirX Identity Customization Guide*.

-  Displays the Help Viewer.
-  After clicking this button, you can click most items in the current view to get help information.

3.2.4. Using Tool Tips

Tool tips provide additional information at various places. A tool tip is typically displayed for about 4 seconds. If you need a longer display time, press the shift key while the tool tip is displayed or move the pointer slightly over the tool tip.

You can enable or disable the tool tip feature from the Views menu.

Tool tips sometimes provide a hint that more information is available. Press the Shift key to display the additional information.

3.2.5. Inactive Objects

Inactive objects are displayed with a dimmed icon in the tree.

3.2.6. Using the Context Menu

DirX Identity Manager provides a context menu that is displayed:

- When you right-click an object in the tree pane or list pane of a Provisioning view or the Connectivity Expert View
- When you right-click a workflow line or a connected directory icon in the Connectivity Global View

The context menu enables only those options that apply to the selected object type; options that do not apply are unavailable.

The following sections summarize the common selections, Provisioning view-specific selections, and Connectivity-view specific selections that can appear in the DirX Identity Manager context menu. See also the "Workflow Line" and "Connected Directory Icon" topics in "Using the Global View" for an explanation of the context menu options available there.

3.2.6.1. Common Context Menu Selections

The following context menu selections can appear in both Provisioning and Connectivity views:

Certificate Change Notification - if you added or exchanged a certificate for attribute and bind profile encryption, this menu option allows you to distribute the new certificate to all applications.

Copy - copies the selected objects with all its content to the clipboard. Use Paste to insert this content at another location. That means that you can use the Copy and Paste sequence to copy objects. Copy together with Paste performs the same operation as **Copy Object** but with different handling. Alternatively you can use the drag and drop feature.

Copy Object - copies the object with all its content. You are asked for the new name (a proposal is presented). Please note that references are not updated automatically. You must perform this task by hand. Copy Object performs the same operation as **Copy** and **Paste** but with different handling. Alternatively you can use the drag and drop feature.

Cut - copies the selected objects with all its content to the clipboard. If you Paste it at the target location, the content at the source location is deleted. That means that you can use a cut-and-paste sequence to move objects. Cut together with Paste performs the same operation as **Move Object** but with different handling. Alternatively you can use the drag and drop feature.

Delete Collection Entries - after explicit confirmation by the user, deletes all entries that are defined by this collection. It deletes the LDAP entries in the following sequence:

1. subtrees in down-up order
2. single objects in down-up order only if they have no children
3. objects defined by rule only if the object has no children
4. subcollections

Down-up order ensures that single objects or subtree lists will be processed in the desired order. For example, suppose we have the following entries in single objects:

cn=d
cn=c, cn=d
cn=b,cn=c, cn=d
cn=a,cn=b,cn=c,cn=d

The Delete action will delete the entire sequence starting from the last object up to the first one.

Note that you can use the Import Collection File method to restore a delete operation *if* you have previously exported the data.

Export Collection - exports the defined collection(s) to the defined LDIF files. This item is only available at the **Collection** object, a selected set of collection objects (use multi selection) or a **Collection Folder**.

Export File - exports objects that contain text data to a text file into the file system. You are asked for the name and location of this file in a file dialog. At the end of the operation, you can view the trace file.

Goto Dataview - displays the selected object in the Data View.

Import Collection File - imports the file of this collection definition from the defined path. The action supports multi selection so that you can import multiple files with one click. It works with these import options: add new entries + modify existing entries + overwrite attribute values. This selection allows easy rollback of a previous **Delete Collection Entries** operation if you exported the file in a previous operation.

Import File - imports text data in a file into an object that contains text data. You are asked for the name and location of the file to import in a file dialog. Do not try to import these files with another mechanism (the internal structure is complex - a lot of special characters are contained).

Load IdS-J Configuration - loads all Java-based workflow definitions into the IdS-J server. The sent message contains the domain name. Depending on the setting of the flag **Include domain into topic** at the domain object, the Java-based Server performs the reload (flag is TRUE) or not (flag is FALSE). It also loads the Java-based schedules and the adaptor configuration. Nothing else is loaded; for example no object descriptions are loaded. Note: This menu option does not load the server configuration. This is only possible during an IdS-J server restart. The algorithm of the domain name calculation depends on where the command is executed:

- From within a Provisioning domain, the domain name is set to the domain's name. The selection is available in the Workflows view.
- From within a Connectivity domain, the domain name is either calculated from the path (for connected directories, workflows, schedules) or from the domain name attribute at the Java-based Server object itself. The selection is available in the Expert View.

Move Object - moves objects between folders. You are asked for the new location. Then a progress dialog is displayed. You should not abort this operation because you can undo it simply by moving the object back to the original location. Move Object performs the same operation as **Cut** and Paste but with different handling. Alternatively you can use the drag and drop feature.

New - creates a new object. If several objects can be created under this object a selection list is displayed in the sub menu.

Open - performs the defined viewer command of the connected directory. In the Connectivity Expert View, this item is only available at the **Connected Directory** object. In the Provisioning view, this selection is only available through the **Connectivity** context menu selection on a target system object. Please note that each **Open** command in the Global View opens another instance of the viewer.

Paste - inserts cut or copied objects from the clipboard (see Cut or Copy). This option is only available if it is allowed to copy these objects to the current location.

Properties - shows the properties of an object in a separate window. You must close this window before you switch to another location in the Expert View.

Refresh - refreshes an object by reading actual data from the configuration database.

Reload Object Descriptors - all object descriptions are read during startup of the DirX Identity Manager. Changes are not reflected automatically to this memory copy. You can restart the DirX Identity Manager or you can use this option to reload the object descriptions after changes.

Rename - renames the object display name (not the common name!) of the object.

Report - generates reports in either HTML or XML format. HTML format is best used for documentation; XML can be used for further processing. For a detailed description of the parameters, see the Reports section in the "Context Sensitive Help" chapter of the *DirX Identity Provisioning Administration Guide*. For information on how to set up your own reports, see the chapter "Customizing Status Reports" in the *DirX Identity Customization Guide*.

Run Workflow - starts a workflow from the Expert View (only available at workflow objects in the Workflows folder) or from the **Connectivity** context menu selection on a target system object in the Provisioning view. A "Run workflow *workflowname*" window is displayed for Tcl-based workflows or a note is displayed that the Java-based was started. Note: You can also start workflows from the Global View context menu (right-click on a workflow line, select a workflow from the context menu, and then click **Run**).

3.2.6.2. Provisioning View Context Menu Selections

The following selections can appear in Provisioning view context menus:

Abort - aborts a request workflow activity if it is in the **WaitInError** state. The resulting state is **Failed.Temporary**. This item is only available on a Request Workflow Instance object.

Connectivity - operates on the connected directory linked to the target system through the Relationship - Connected Directory link. The selection provides options to configure and open the connected directory or to add or assign new workflows. You can also run workflows. DirXmetaRole represents the Identity Store connected directory.

Delete - deletes the object. The selection displays a confirmation dialog that asks you whether or not you really want to delete this object. Because the object may still contain history (audit) information or may be protected by request workflows for deletion, the object is only deleted after an object-specific procedure. For more information, see the *DirX Identity Provisioning Administration Guide*.

Export Nationalization Items - exports all nationalization items within the selected tree into a nationalization file. This selection is available in the Domain view and the Workflows view.

Login/Logout - creates a new instance of a Provisioning view or a Data View and authenticates you to this instance, or logs you out of an instance of a view. The DirX Identity login dialog is displayed (See "Logging In" for details). This menu selection allows you to run

multiple instances of Provisioning views or Data Views. It is available at the top-level trees of Provisioning views and Connectivity and Provisioning Data Views.

Resume - triggers the request workflow engine to run this activity again. Either the activity runs successfully or enters the state **WaitInError** again. This item is only available on a Request Workflow Instance object that is in state **WaitInError**. This selection is available in the Workflows view.

3.2.6.3. Connectivity View Context Menu Selections

The following selections can appear in Connectivity view context menus:

Configure - starts the connected directory configuration wizard or the configuration wizard for the workflow for reconfiguration. This item is only available at the **Connected Directory** and **Workflow** object in the Global View and Expert View.

Delete - deletes the object. The selection displays a confirmation dialog that asks you whether or not you really want to delete this object. You can also select whether or not the deletion process should check for references to avoid broken links (**Check references to avoid broken links**). When references are detected, a confirmation dialog is displayed and deletion is not performed. We recommend that you use the checked option. The first use during a session needs more time, repeated use works much faster due to caching mechanisms. You can use the **Show References** menu option to test for references before a deletion operation. Please note that no undo is available. We recommend that you make regular backups of your configuration database.

Disable Scheduling - disables the scheduling mechanism previously enabled with **Enable Scheduling** (enabled from C++-based server startup). You can use this option to disable all schedules (running workflows are not aborted!). After checking with **Get Server State** that no workflows are running on any of the servers, you can be sure that no automatic activity can occur. You should use this option before restoring the database or when using complex operations like **Import Data**. This item is only available at the **Schedules** object in the Expert View.

Edit Content - allows editing the XML content of this object directly. After editing it is stored directly in LDAP and is not interpreted by the service layer (which could adapt the result).

Enable Scheduling - enables the scheduling mechanism previously disabled with **Disable Scheduling**. This item is only available at the **Schedules** object in the Expert View.

Export Configuration - exports the entire configuration tree into an LDIF file. You can read this information with **Import Data**. This feature permits you to make backups of the configuration tree. This item is only available at the root object **Connectivity Configuration Data**. If an error occurs, a dialog is displayed at the end of the operation. You can also view the trace file.

Export Data - exports complete logical trees of data from the configuration database to an LDIF file. You are asked for the name and location of the file to export in a file dialog. If an error occurs, a dialog is displayed at the end of the operation. You can also view the trace file.

Note: The default code set is utf-8 (the scripts support the switch -code <encoding>).

Export Subtree - exports the selected object and all of its children in the tree from the configuration database to an LDIF file. You are asked for the name and location of the file to export in a file dialog. If an error occurs, a dialog is displayed at the end of the operation. You can also view the trace file.
Note: The default code set is utf-8 (the scripts support the switch -code <encoding>).

Get Server State - displays the server state of a C++-based Server object (only available at this object).

Import Data - imports data that has been exported to LDIF format with **Export Data** or **Export Configuration**. This item is only available at the root object **Connectivity Configuration Data**. The imported data does not delete objects, it only adds and modifies them. If you want to replace the entire configuration tree, use **Replace Configuration** instead. If an error occurs, a dialog is displayed at the end of the operation. You can also view the trace file.

The default code set is utf-8 (the scripts support the switch -code <encoding>).

Manage IdS-J Configuration - allows specifying static load distribution. You can define specific adaptor types, where the scheduler and the request workflow timeout check run, and, for high availability, which server supervises which server.

Replace Configuration - imports data that has been previously been exported to LDIF format with **Export Configuration**. Before the import operation is started, the configuration tree is deleted (only the configuration objects that keep important configuration information for the local DirX Identity domain are not touched). This item is only available at the root object **Connectivity Configuration Data**. At the end of the operation a dialogue is displayed when an error happened. You can also view the trace file.

Replace Occurrences - maps all links that point to the selected object to a new one that you can select from a tree browser.
Note: This command does not copy the attributes of the source object to the target object. You must do this by hand if necessary.

Run Activity - runs a workflow from any activity. Be sure that all input conditions for this activity are satisfied, for example, an intermediate file must be present in the working directory of the previous activity. This item is only available at the root object **Activity** object under a **Workflow** object.

Show References - checks whether other objects refer to a specific object. This selection helps to maintain the database while avoiding broken references. Note that you can use this feature in the **Delete** menu option. The next figure shows a typical situation.

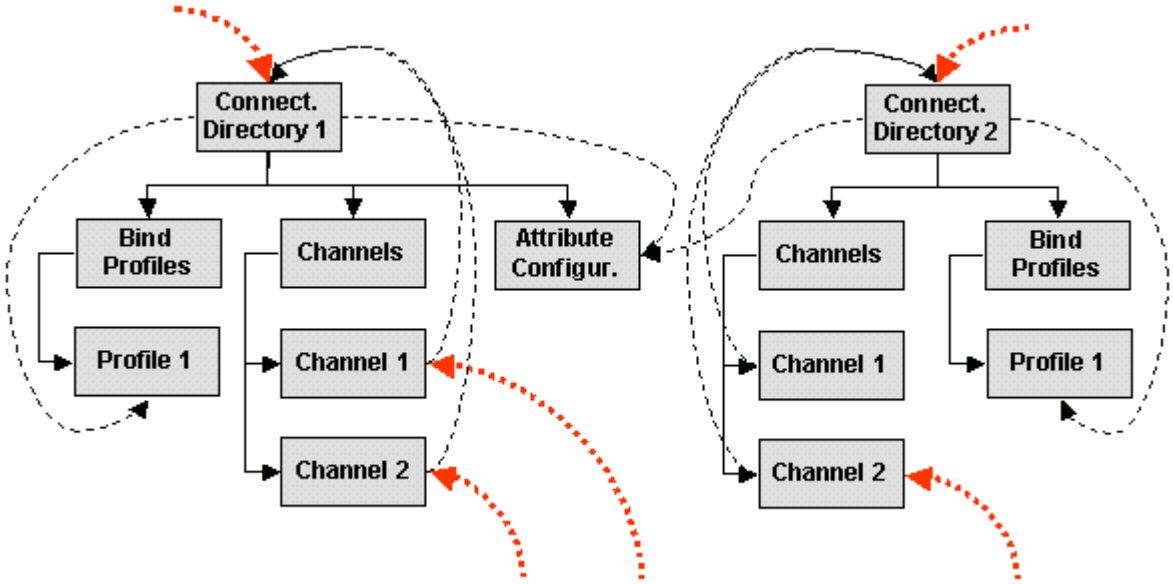

Figure 15. Showing Object References

The figure shows two selected objects (Connected Directory 1 and 2). Both objects have sub structures as there are bind profile folders with bind profiles and channel folders with channels.

The connected directories refer to their bind profiles and to the same shared attribute configuration object. The channels refer back to the connected directory objects. External references (thick dotted lines) refer to channel and connected directories. Thus deletion of both connected directory objects together with their subtrees would lead to 5 broken references. The secure method is to remove the external references, to check that they no longer point to these objects and then to delete the object trees.

The show references method has two options:

- **Include objects referring to any children** - References to the selected objects as well as to their children will be searched (external references).
- Ignore ancestor / descendants references - This option ignores:
  - references of the selected objects (ancestor) to their children (for example the references to the bind profiles).
  - references of children to their ancestor (for example the references from the channels to the connected directories).
  - references of the children to other children of the respective ancestor

In other words: When this option is checked, only references from “outside” to the selected object (external references) are taken into account. To find out if an object may be deleted without corrupting the database, check both options.

Show Structure - displays the structure of a workflow object from the Expert View (only available at workflow objects in the Workflows folder).

Synchronize Schedulers - synchronizes the current schedules information to all schedulers (for example, after a reload of the configuration database). Interactive changes of a

schedule object should be synchronized automatically. This item is only available at the **Schedules** folder in the Expert View.

3.2.7. Using Drag and Drop

In all views that provide a tree you can use DirX Identity's drag and drop feature:

- Simply select one or more objects.
- Click on the selection with the left mouse button and then move the cursor. A dashed grey rectangle under the cursor shows that you move the selection.
- If you move the cursor over a potential target location, either the target location is highlighted in blue (this is a valid one) or a stop sign shows that you cannot use it.
- Pressing the **Ctrl** key defines a Copy operation (a plus sign is displayed below the cursor). If you do not press another key, a **Move** operation is performed.
- If you release the left mouse button, the copy or move operation is performed.
- To abort a drag and drop operation, simply move the cursor to a location where the stop sign is displayed and then release the mouse button.

For alternative methods for Copy or **Move**, see the corresponding menu items.

3.2.8. Using the Status Bar

The status bar at the bottom of the window contains valuable information:

- The host name where this manager is connected to (the LDAP server host name).
- The logged-in user.
- The number of items visible under the currently selected tree node that is typically shown as a list in the upper right pane.

3.3. Supplying Date and Time

Some fields in DirX Identity allow input of date and time.The format is set to English and is currently not changeable.Thus the date format is:

English: 4/12/01 0:47 am

3.4. Managing Your Configuration Database

If you need to restore or exchange the database that contains your configuration, follow these steps:

1. Use **Disable Scheduling** (an option in the Schedules object in the Expert View) to prevent workflows from being started automatically.For details, see "Connectivity View Context Menu Selections".
2. Stop the DirX Identity IdS-J service.(Stops all Java-based Servers.)

3. Use **Get Server State** to check, for all C++-based Servers, that no workflows are still running.For details, see "Connectivity View Context Menu Selections".
4. Stop the DirX Identity IdS-C service.(Stops all C++-based Servers.)
5. Restore your database.You should be careful not to restore a database with an incompatible schema version.DirX Identity will not restart if this occurs, and you cannot use DirX Identity Manager on the database.In this case, you must migrate the database (assuming that the database version is one of the supported versions for migration).
6. Restart the DirX Identity Manager.
7. Start the DirX Identity IdS-C service.(Start all C++-based Servers.)
8. Start the DirX Identity IdS-J service.(Starts all Java-based Servers.)
9. Use **Enable Scheduling** (an option in the Schedules object in the Expert View) to re-start automatic workflow launch again.For details, see "Connectivity View Context Menu Selections".

If you do not follow this sequence, an inconsistent database could be the result.

3.5. Handling Erroneous Field Content

When fields in list boxes look like **ABC??**, it indicates that the value is no longer part of the selection list.This can happen especially when the selected attributes are used for list boxes.Either select another value for the list box or change the content of the list by editing the source (for example, the selected attributes).

3.6. Using Wizards

DirX Identity wizards are powerful, easy-to-use tools that help to simplify complex configuration tasks and enable you to concentrate on the important parts of a configuration.DirX Identity Manager provides the following built-in wizards for setting up configuration scenarios:

- One Provisioning target system wizard for creating and configuring target systems that is available in the Provisioning Target Systems view
- Two Connectivity wizards - one for creating and configuring connected directories and one for creating and configuring workflows between connected directories - that are available in the Connectivity Global View

These wizards isolate the most important configuration tasks of setting up a synchronization workflow and bring them into a logical sequence.

3.6.1. About the Wizard Page Layout

The configuration wizards follow a predefined layout. They start as modal dialog windows that display a form dialog called a wizard panel. The wizard panel consists of the following elements:

- **Title** (for example, "Select attribute configuration").

- **Description** (for example, "Check if the attribute items shown here are appropriate for a synchronization procedure. Update if necessary. Then click on "Next>>" to perform the next step.")
- **Progress illustrator**, which indicates the steps that you have already performed (green color), the current step (grey color), and the steps that remain to be performed (red color). For the Connectivity wizards, the items are displayed as buttons when the respective object (connected directory or workflow) is re-configured. Click on a button to jump to the corresponding step directly.
- **Work area**. Displays the input dialog for the current step.
- **Navigation buttons**:
- **<< Previous** - steps backward (disabled for the first step).
- **Next >>** - steps forward (labeled **Finish** >> for the last step).
- **Cancel** - stops the wizard.
- **Help** - provides help information for this step.

3.6.2. How the Target System Wizard Works

You can use the Provisioning view's Target System wizard to create new target system objects (you cannot use it to re-configure a target system object). This wizard provides for complete configuration of a new target system, including both the Connectivity and Provisioning pieces of the new system.

When you run the Target System wizard, it first requires you to select a pre-configured target system. The wizard derives the new target system from this template. The wizard also provides steps to:

- Provide a name for the new target system and assign it an administrator
- Select the cluster and domain and specify any assignment properties, synchronization properties, and group handling properties
- Define the timing (in days) as to when target system objects are disabled or deleted
- Configure account and group roots
- Select the Connectivity scenario and the connected directory, and configure the connected directory
- Select the Provisioning workflows to create, for example, Java-based or Tcl-based versions

Parts of the Target System wizard are customizable; see the chapter "Customizing Wizards" in the *DirX Identity Customization Guide* for details.

3.6.3. How the Connectivity Wizards Work

You can use the Connectivity wizards to create new objects or to re-configure existing ones. The steps you take in the wizard are different depending on which task you are performing and the kind of object you are creating or re-configuring:

1. When you create a new object, you must first select a template. When you are re-configuring an existing object, the wizard does not show you this step.
2. The next steps in the wizard depend upon the type of object you are configuring.
3. When you create a new object, you must define a name for it as the last step in the wizard. When you are re-configuring an object, the wizard does not show you this step.
4. When you want to re-configure a connected directory or a workflow using a particular step, you can jump to the desired step directly by clicking the step in the progress illustrator.

When you use the Connected Directory Configuration wizard to create a new connected directory or to insert an existing connected directory, you must first select a pre-configured connected directory. The wizard derives the new directory from this template. In most cases, you must only check whether or not the current settings are correct and adjust them if necessary. The following items are typical for this type of wizard but not always available:

- Select the connected directory template (only when creating a connected directory object)
- Select the schema settings
- Select the attribute configuration settings
- Check the login (bind) profiles and create new ones if necessary.
- Provide a name for the new connected directory (only when creating a connected directory object).

When you use the Workflow Configuration wizard to create a new workflow, the wizard presents all workflows that fulfill the condition to connect the two directory types at the endpoints and therefore fit between the two (each of these workflows acts as a template). The list shows only those workflows that apply to the selected connected directories (that is, the source and target directories between which you've drawn the workflow line). If a template for the two connected directories does not exist, you must create one in the Expert View. The following items are typical for this type of wizard but not always available:

- Select a workflow template (only when creating a new workflow)
- Select the attributes to extract from this connected directory
- Select the attributes in the target connected directory which must be filled
- Define the mapping between the source and target attributes
- Set the search parameters or, more generally, the export parameters for the source connected directory
- Set the object handling for the import of the target attributes (that is, which objects can be deleted or created) or, more generally, the import parameters for the target connected directory
- Set the delta handling parameters if this is a delta workflow
- Adjust the trace parameters (eventually separate for each of the agents)
- Provide a name for the workflow (only when creating a new workflow).Next time you run the wizard, it will present this new configured workflow as a template when a new

workflow must be configured between these types of directories.

The Connectivity wizards are customizable; see the chapter "Customizing Wizards" in the *DirX Identity Customization Guide* for details.

3.7. Using the Provisioning Views

When you select the Provisioning view group, the view bar in the main window displays icons that allow you to select the following views:

- Users
- Business Objects
- Tickets
- Privileges
- Policies
- Certification Campaigns
- Workflows
- Target Systems
- Auditing
- Domain Configuration

Each view presents a tree pane and a search pane on the left side of the main window and a list pane and a details pane on the right side of the main window.

The tree pane displays a hierarchical tree of the objects that you are allowed to manage in this view and (depending on the view) set of pre-configured query folders that can be used to define individual views of the objects in the tree. To display this pane, click the Tree tab.

When managing objects you can specify a due date for creating, modifying or deleting of most object types. If this date is not in the past a ticket with the corresponding order is created.

The search pane provides a dialog for selecting and displaying a subset of the objects available in this view group. To display this pane, click the Search tab.

The list pane displays the properties of an object selected in the tree pane in column format. It appears in the upper right-hand side of the main window.

The details pane displays the properties of an object selected in the tree pane or the list pane in tabbed format. It appears in the lower right-hand side of the main window. Click the tabs to view and edit the object’s properties.

For detailed information about the panes presented in the Provisioning view groups, see the "Core Component" section in the DirX Identity Manager online help. The remainder of this section provides a brief description of how to work with the Provisioning view.

3.7.1. Using the Users View

The tree pane in the Users view displays the following items:

- A tree of user entries organized into a hierarchy of "ordering" folders, including folders for countries, domain components, localities, organizations (departments), and organizational units (teams). By default, an individual user is displayed as "surname given name", for example, "Farfello Nico". The Users view tree pane is completely customizable. You can use the context menu to create your own organization subfolders (representing departments) and organizational unit subfolders (representing teams) to hold user entries, and you can create your own subtree of domain components (country, locality, and so on). You can also change the way in which user objects are displayed in the tree by changing the display name attribute for the user object type; by default, "cn" (common name) is specified as the display name attribute, but you can define another display name attribute for the user type (as well as other object types) in the object descriptions. For more information, see the section "Changing the Display Name of Entries in the Provisioning Tree View" in the *DirX Identity Customization Guide*.
- A set of query folders for filtering a set of user entries according to various criteria. In the Users view, query folders allow you to search for and identify users that need some administrative action to be taken. The default query folders supplied by DirX Identity (for example, "Errors", "Inconsistent" and "To Be Deleted") address some common user administration tasks. You can also use the context menu to create your own query folders or copy a default query folder and change its properties to your requirements. You can find detailed information about how to create query folders in the topic "Creating a Query Folder" in the "Core Components" section of the DirX Identity Manager online help. For more information on user query folders, see the *DirX Identity Provisioning Administration Guide*.

The Search pane dialog (click the Search tab) in the Users view allows you to select and display a subset of the users in the tree pane or locate a specific user in the tree. This dialog is especially useful for performing user management tasks in extremely large user databases. You can find detailed information about the Search pane dialog in the "Core Components" section of the DirX Identity Manager online help.

For more information about the context menu selections that may be available in this view, see the topic "Using the Context Menu". For more information about the properties of objects displayed in the Users view, see the context-sensitive help. For information about user management tasks and how to accomplish them with DirX Identity Manager, see the chapter "Managing Users" in the *DirX Identity Provisioning Administration Guide*.

3.7.2. Using the Business Objects View

The tree pane in the Business Objects view (click the Tree tab) displays hierarchical trees of business objects. DirX Identity provides the following default business object trees:

- The Companies tree, which you can use to model your company’s organizational structure. Right-clicking on the top level of the tree allows you to use the **New** context menu selection to create additional company container folders and new nodes in the tree (Organization business objects). Right-clicking a node in the tree allows you to use

the **New** context menu selection to create Organization and Organizational-Unit business object types or generic-structure business objects (use the Context selection).

- The Cost-Units tree, which you can use to model your company's cost-unit structure and cost-center information. Right-clicking on the top level of this tree allows you to use the **New** context menu selection to create additional cost-unit container folders and new nodes in the tree (Cost-Unit business objects). Right-clicking a node in the tree allows you to use the **New** context menu selection to create Cost-Unit business object types or generic-structure business objects (use the Context selection).
- The Countries tree, which you can use to model your company's regional distribution. Right-clicking on the top level of this tree allows you to use the **New** context menu selection to create additional country container folders and new nodes in the tree (Country business objects). Right-clicking on a node in the tree allows you to use the **New** context menu selection to create Location business objects types or generic-structure business objects (use the Context selection).
- The Projects tree, which you can use to define the various projects running in your organization. Right-clicking on the top level of the tree allows you to use the **New** context menu selection to create additional project container folders and new nodes in the tree (Project business objects). Right-clicking on a node in the tree allows you to use the **New Project** menu selection to create Project business objects.

DirX Identity also provides a "Custom" business object tree. Use this tree to create your own business object types (use the **New** → **Context** selection from the context menu).

The search pane dialog in the Business Objects view (click the Search tab) allows you to select and display a subset of the business objects available in the tree pane or locate a specific business object in the tree. You can find detailed information about the Search pane dialog in the "Core Components" section of the DirX Identity Manager online help.

For more information about the context menu selections that may be available in this view, see the section "Using the Context Menu". For more information about the properties of objects displayed in the Business Objects view, see the context-sensitive help. For information about business object types, business object management tasks and how to accomplish these tasks with DirX Identity Manager, see the chapter "Managing Business Objects" in the *DirX Identity Provisioning Administration Guide*.

3.7.3. Using the Tickets View

The tree pane in the Tickets view (click the Tree tab) displays the Tickets tree. The Ticket tree displays the following sub trees:

- The Internal tree, which contains the tickets that the DirX Identity built-in ticket mechanism creates when specifying a due date in the future while managing objects, for example users or business objects. The Internal tree displays the following sub trees and folders:
- The _Queries tree, which contains a set of default queries for filtering the tickets in the Internal tree according to various criteria. You can use the queries in this tree to search the Internal tree for tickets with a specific status, for active tickets, for error tickets and processed tickets, for tickets with time constraints, and for tickets that perform specific

operations on specific object types. You can also use the context menu to create your own query folders or copy a default query folder and change its properties to your requirements. For detailed information about using query folders, see the topic "Creating a Query Folder" in the "Core Components" section of the DirX Identity Manager online help.

- A folder for each object type, for example **Users**, **Roles**, and so on. Under each of these type folders there are folders indicating the due dates, for example **2011-09-05**. These date folders contain the ticket objects.
- Other trees, which contain custom tickets for completely customer defined objects and processes. The sub structure of this tree is completely dependent of the custom solution.

The Search pane dialog (click the Search tab) in the Tickets view allows you to select and display a subset of the tickets in the tree pane or locate a specific ticket in the tree. You can find detailed information about the Search pane dialog in the "Core Components" section of the DirX Identity Manager online help.

For more information about the context menu selections that may be available in this view, see the topic "Using the Context Menu". For more information about the properties of objects displayed in the Tickets view, see the context-sensitive help. For information about ticket management tasks and how to accomplish them with DirX Identity Manager, see the chapter "Managing Tickets" in the *DirX Identity Provisioning Administration Guide*.

3.7.4. Using the Privileges View

The tree pane in the Privileges view (click the Tree tab) displays hierarchical trees of privilege objects. DirX Identity provides the following privilege object trees:

- The Roles tree, which presents a hierarchical tree of the roles defined for the domain and a set of default query folders for filtering them according to various criteria. Right-clicking on a container in the tree allows you to use the **New** context menu selection to create additional role container folders, role objects or query folders. Note that the Roles tree is only available if the optional Pro Suite is installed, which requires an additional license.
- The Permissions tree, which presents a hierarchical tree of the permissions defined for the domain and a set of default query folders for filtering them according to various criteria. Right-clicking on a container in the tree allows you to use the **New** context menu selection to create additional permission container folders, permissions objects or query folders. Note that the Permissions tree is only available if the optional Pro Suite is installed, which requires an additional license.
- The Groups tree, which is a virtual tree of the groups defined for each target system that is also visible in subfolders within the Target Systems view. The Groups tree consists of a set of target system objects- each object contains the groups defined for that target system - and a tree of default query folders for filtering them according to various criteria. Default query folders are also available within each target system object. Right-clicking on the top-level Queries folder allows you to use the **New** context menu selection to create new target system container folders, target system objects, and query folders. Right-clicking on a target systems object loads the menus for the

associated connected directory and its workflows from the Connectivity side. Right-clicking on a group subfolder (container) within a target systems object allows you to use the **New** context menu selection to create a new group subfolder, a new group or a new query folder. Right-clicking on a group allows you to create a new group (use the **New Group** selection) to build hierarchical group structures.

In the Privileges view, query folders allow you to search for and identify privilege objects that need some administrative action to be taken. The default query folders supplied by DirX Identity address some common privilege administration tasks. You can also use the context menu to create your own query folders or copy a default query folder and change its properties to your requirements. For detailed information about using query folders, see the topic "Creating a Query Folder" in the "Core Components" section of the DirX Identity Manager online help. For more information on using privilege object query folders, see the section "Working with Privilege Structure Query Folders" in the *DirX Identity Provisioning Administration Guide*.

The search pane dialog in the Privileges view (click the Search tab) allows you to select and display a subset of the privilege objects available in the tree pane or locate a specific privilege object in the tree. You can find detailed information about the Search pane dialog in the "Core Components" section of the DirX Identity Manager online help.

For more information about the context menu selections that may be available in this view, see the topic "Using the Context Menu". For more information about the properties of objects displayed in the Privileges view, see the context-sensitive help. For information about privilege management tasks and how to accomplish them with DirX Identity Manager, see the chapter "Managing the Privilege Structure" in the *DirX Identity Provisioning Administration Guide*.

3.7.5. Using the Policies View

In the Policies view, the tree pane (click the Tree tab) displays two trees:

- The Policies tree, which contains the policies and rules for access control and automated provisioning as well as segregation of duties (SoD) and password policies.
- The Delegations tree, which contains the delegations created with DirX Identity Web Center.

The search pane (click the Search tab) allows you to select and display a subset of the policy objects available in the tree pane or locate a specific policy object in the tree.

The Policies tree consists of a set of subtrees that correspond to the types of policies available for creation and a tree of query folders for filtering the objects in the Policies tree according to various criteria. Right-clicking on the top-level node in the tree allows you to create new containers for each type of policy available in the tree, new query folders, and new generic containers.

The structure of each policy-type subtree depends on its type. Most subtrees provide a subfolder that contains the default policies that apply to this type of policy, and one or more domain-specific subfolders that contain customized policies. Right-clicking on the subtree or its subfolders allows you to use the **New** context menu selection to create a new

container folder or policy for this type.

In the Policies tree, query folders allow you to search for and analyze instances of user access to specific resources. For more information on how to use query folders in the Policies tree, see the section "Verifying Access Policies" in the *DirX Identity Provisioning Administration Guide*.

The Delegations tree provides a way to view the delegations created in DirX Identity Web Center from DirX Identity Manager. The Delegations folder itself is never populated with entries. The Access Rights subtree presents all of the possible operations (for example, approve, grant, modify, and so on) that can be executed on all of the possible object types. The Access Rights subtree is initially empty; over time, it becomes populated with records of the access rights delegations that are made from one user to another in the Web Center.

For more information about the context menu selections that may be available in this view, see the topic "Using the Context Menu". For more information about the properties of objects displayed in the Policies view, see the context-sensitive help. For information about delegated administration, policy management tasks and how to accomplish them with DirX Identity Manager, see the *DirX Identity Provisioning Administration Guide*.

3.7.6. Using the Certification Campaigns View

In the Certification Campaigns view, the tree pane (click the Tree tab) displays tree of certification campaign objects. Certification campaigns tree also has two predefined containers under its root:

- _Default, which contains notification templates usable as baseline for customized notifications in user defined certification campaigns.
- _Queries, which is prepared for user-defined query folders and by default is empty.
- _Archive, which contains past and successfully finished certification campaigns for campaigns with **Recurring Certification Campaign** set. By default, this folder is not available and is created when a recurring campaign restarts.

The search pane (click the Search tab) allows you to select and display a subset of the certification campaign objects available in the tree pane or locate a specific certification campaign object in the tree.

Certification campaign objects in the tree are represented by name and state of the campaign. Each object has two subfolders: one for notifications and other for items certified in the campaign. You can create new notifications in Notifications subfolder with the context menu.

Right-clicking on Certification Campaigns or any container folder allows you to use the **New** context menu selection to create a new Certification campaign object, container or query folder.

For more information about the context menu selections that may be available in this view, see the topic "Using the Context Menu". For more information about the properties of objects displayed in the Certification Campaigns view, see the context-sensitive help. For more information about user certification campaigns and how to work with them in DirX

Identity Manager, see the Use Case Document *DirX Identity User Certification Campaigns*.

3.7.7. Using the Workflows View

In the Workflows view, the tree pane (click the Tree tab) displays the following subtrees:

- The _Queries tree, which contains a set of default queries for filtering the workflow definitions in the Definitions tree according to various criteria. You can use the queries in this tree to search the Definitions tree for active and inactive workflows and for workflows that perform specific operations on specific object types. You can also use the context menu to create your own query folders or copy a default query folder and change its properties to your requirements. For detailed information about using query folders, see the topic "Creating a Query Folder" in the "Core Components" section of the DirX Identity Manager online help. For more information about using the request workflow query folders in this tree, see the section "Managing Request Workflow Definitions" in the *DirX Identity Provisioning Administration Guide*.
- The Configuration tree, which contains configuration objects that allow you to set global parameters and services that can be used by the request workflow definitions. Right-clicking on the items in this tree allows you to use the **New** context menu to create new activity types (Component description objects), new common activities (Message item objects), and new services (Services and SMTP services objects). For more information on how to use the items in this tree, see the section "Managing Configuration Objects" in the *DirX Identity Provisioning Administration Guide*.
- The Definitions tree, which contains a subfolder of default request workflow definitions, one or more domain-specific subfolders that contain customized request workflow definitions, and a System subfolder that contains system-wide workflows, for example, a standard workflow that sends all electronic mail items. Right-clicking on the default and the domain-specific subtrees allow you to use the **New** context menu selection to create new workflow container folders and workflows. For more information about using the items in this tree, see the section "Managing Request Workflow Definitions" in the *DirX Identity Provisioning Administration Guide*.
- The Monitor tree, which contains entries that reflect running and completed workflows and a set of default queries that allow you to search for and display various subsets of these entries. For more information on how to use the items in this tree, see the section "Managing Request Workflow Instances" in the *DirX Identity Provisioning Administration Guide* and the section "Getting Status and Debugging Information from the Monitor Views" in the *DirX Identity Troubleshooting Guide*. This tree also contains the Delta subtree, which holds delta status entries of Java-based delta workflows. For a general explanation of the delta workflows, see the relevant sections in the chapter "Java-based Workflow Architecture" in the *DirX Identity Application Development Guide*.

The search pane dialog in the Workflows view (click the Search tab) allows you to select and display a subset of the request workflow objects available in the tree pane or locate a specific object in the tree. You can find detailed information about the Search pane dialog in the "Core Components" section of the DirX Identity Manager online help.

For more information about the context menu selections that may be available in this view, see the topic "Using the Context Menu". For more information about the properties of

objects displayed in the Workflows view, see the context-sensitive help. For information about request workflow management tasks and how to accomplish them with DirX Identity Manager, see the chapter "Managing Request Workflows" in the *DirX Identity Provisioning Administration Guide*.

3.7.8. Using the Target Systems View

The tree pane in the Target Systems view (click the Tree tab) displays a hierarchical tree of the target systems whose access control information has been imported into the Provisioning configuration of the Identity Store. The Target Systems tree consists of a set of target system objects and a tree of default query folders for filtering the objects in the target system tree according to various criteria. Right-clicking on the top-level node in the tree allows you to use the **New** context menu selection to create new cluster containers, target system containers, query folders, and target systems. Right-clicking on the _Queries folder allows you to use the **New** context menu selection to create new query folders, target system containers, and target systems.

Each target system object contains the following subfolders:

- An Accounts folder, which contains the target system accounts and a set of account-specific query folders. This subfolder is only present when the target system requires the management of accounts. Right-clicking on this folder allows you to use the **New** context menu selection to create a new container folder, a new account, or a new query folder.
- A Groups folder, which contains the target system's groups and set of group-specific query folders. Right-clicking on this folder allows you to use the **New** context menu selection to create a new container folder, a new group, or a new query folder.

Note that accounts and groups can be contained in a single subfolder if the target system was configured this way.

- A Configuration folder, which contains the following subfolders:

A JavaScripts folder, which stores the Java scripts that are referenced from within the object descriptions.

An Object Descriptions folder, which stores the object descriptions for the target system's accounts and groups.

An Obligations folder, which contains common On Assignment, On Revocation and On Validation rules that can be used by many group objects.

A folder for storing Proposal Lists.

A folder for storing specifications for the generation of reports about the target system's accounts and groups.

(Optional) a Delta folder, which contains the delta status entries of cluster workflows. For a general explanation of the delta workflows, see the relevant sections in the chapter "Java-based Workflow Architecture" in the *DirX Identity Application Development Guide*.

Right-clicking on one of the Configuration subfolders allows you to use the **New** context menu selection to create a new configuration object of the type stored in that folder; for example, right-clicking the JavaScripts folder allows you to create a new JavaScript.

In the Target Systems view, query folders allow you to search for and identify target system-related objects that need some administrative action to be taken; for example, finding accounts or groups that require manual administrative follow-up. DirX Identity supplies a set of default query folders that address some common target system administration tasks. You can also use the context menu to create your own query folders or copy a default query folder and change its properties to your requirements. For detailed information about using query folders, see the topic "Creating a Query Folder" in the "Core Components" section of the DirX Identity Manager online help. For more information on target system query folders, see the section "Managing Target Systems" in the *DirX Identity Provisioning Administration Guide*.

The search pane (click the Search tab) in the Target Systems view allows you to select and display a subset of the objects available in the tree pane (in this case, accounts, groups, or target systems) or locate a specific object in the tree. You can find detailed information about the Search pane dialog in the "Core Components" section of the DirX Identity Manager online help.

For more information about the context menu selections that may be available in this view, see the topic "Using the Context Menu". For more information about the properties of objects displayed in the Target Systems view, see the context-sensitive help. For information about target system management tasks and how to accomplish them with DirX Identity Manager, see the *DirX Identity Provisioning Administration Guide*.

3.7.9. Using the Auditing View

The tree pane in the Auditing view (click the Tree tab) displays two trees:

- The Status Reports tree, which contains configuration objects for obtaining information about the current status of DirX Identity objects
- The Audit Trail tree, which contains configuration objects for obtaining historical information about DirX Identity objects

The Status Reports tree consists of two subfolders: a Default subfolder that contains the default status reports provided by DirX Identity and a Customer-Specific subfolder where you can create your own status reports so that they will not be overwritten by new DirX Identity releases. When you right-click on either subfolder, you can use the **New** context menu selection to create new status report containers, reports, or report templates. You can use the **Copy Object** context menu selection to copy a default status report from the Default subfolder to the Customer-Specific subfolder and change its properties to your requirements. For detailed information about creating and changing status reports, see the *DirX Identity Customization Guide*.

The Audit Trail tree provides an Audit Policies subtree that contains the following subfolders:

- The _Queries folder, which contains a set of default query folders supplied with DirX

Identity for filtering the auditing policy objects according to various criteria; for example, to display all active or inactive audit policies.

- The Default audit policies folder, which contains the default audit trail policies for auditing DirX Identity objects provided by DirX Identity
- One or more domain-specific audit policy folders, which contain customized audit trail policies for auditing DirX Identity objects. Use this area of the Audit Policies tree to store your own audit trail policies and audit query folders so that they will not be overwritten by new DirX Identity releases.

Right-clicking on any of these folders allows you to use the **New** context menu selection to create new audit trail folders, query folders, and audit trail policies. You can use the **Copy Object** context menu selection to copy a default audit trail policy or query folder and change its properties to your requirements. For detailed information about using query folders, see the topic "Creating a Query Folder" in the "Core Components" section of the DirX Identity Manager online help. For more information about audit trail policies, see "Managing the Audit Trail" in the *DirX Identity Provisioning Administration Guide*.

The search pane dialog in the Auditing view (click the Search tab) allows you to select and display a subset of the auditing configuration objects available in the tree pane (in this case, auditing policies or status reports) or locate a specific auditing object in the tree. You can find detailed information about the Search pane dialog in the "Core Components" section of the DirX Identity Manager online help.

For more information about the context menu selections that may be available in this view, see the topic "Using the Context Menu". For more information about the properties of objects displayed in the Auditing view, see the context-sensitive help. For information about auditing management tasks and how to accomplish them with DirX Identity Manager, see the chapter "Managing Auditing" in the *DirX Identity Provisioning Administration Guide*.

3.7.10. Using the Domain Configuration View

The tree pane in the Domain Configuration view (click the Tree tab) displays the configuration data that is specific to the customer domain, and is structured as follows:

- The top-level node represents the domain object, from which you can make domain-wide settings such as enabling SoD checking and auditing.
- The trees underneath the domain object contain configuration data that is common to the entire domain, such as template object and property page XML descriptions, target system definitions, JavaScripts, proposal lists, reports, collections, and language-dependent messages.
- The DomainAdmin user object represents the domain administrator that the DirX Identity Provisioning system creates by default.

The search pane (click the Search tab) allows you to select and display a subset of the domain configuration objects available in the tree pane or locate a specific object in the tree.You can find detailed information about the Search pane dialog in the "Core Components" section of the DirX Identity Manager online help.

For more information about the context menu selections that may be available in this view, see the topic "Using the Context Menu".For more information about the properties of objects displayed in the Domain Configuration view, see the context-sensitive help.For information about domain management tasks and how to accomplish them with DirX Identity Manager, see the chapter "Managing Domains" in the *DirX Identity Provisioning Administration Guide*.

3.8. Using the Connectivity Views

The Connectivity view group consists of the following views:

- The **Global View** is the most popular Connectivity view.You should use the Global View if you are a less experienced DirX Identity administrator.The Global View provides wizards to guide you through the synchronization setup procedures and provides selections for performing operation tasks like starting, monitoring or stopping workflows.The Global View hides the complexity of configuration data and flexibility as long as you do not need to perform any low-level object configuration and your configuration procedures consist mainly of the setting of server addresses and attribute mappings.
- The **Expert View** allows you to perform all of the complex configuration work that is necessary for more sophisticated Connectivity configuration solutions.The Expert View provides property dialogs that give you access to all of the details of all Connectivity configuration objects and their properties.Through the Expert View, you can use DirX Identity Manager to configure every aspect of DirX Identity Connectivity and create new synchronization workflows.You can also use the Expert View to add your own connected directories and agents to the Connectivity configuration so that their properties are available for access with the DirX Identity Manager.See the chapter "Customizing Objects" in the *DirX Identity Customization Guide* for more information.
- The **Status Reports** view provides a set of pre-configured status reports for you to copy and tailor to your requirements.
- The **Monitor View** allows you to supervise the results of all the workflow runs of the different synchronization scenarios.It displays a tree that lists the results of all workflows and the activities contained in these workflows.The **process table** allows you to view currently running workflows.

The next sections describe how to use each view.

3.8.1. Using the Global View

The Global View provides a high-level representation of the current DirX Identity Connectivity configuration that is easy to use and hides all complexity of the system that is not necessary for standard configuration tasks. The Global View initially shows a scenario tree and a map with icons and lines. Each icon represents a connected directory. Each line represents a synchronization workflow. This configuration is called a workflow scenario. DirX Identity Manager and the configuration can maintain multiple workflow scenarios. The following figure shows the Global View.

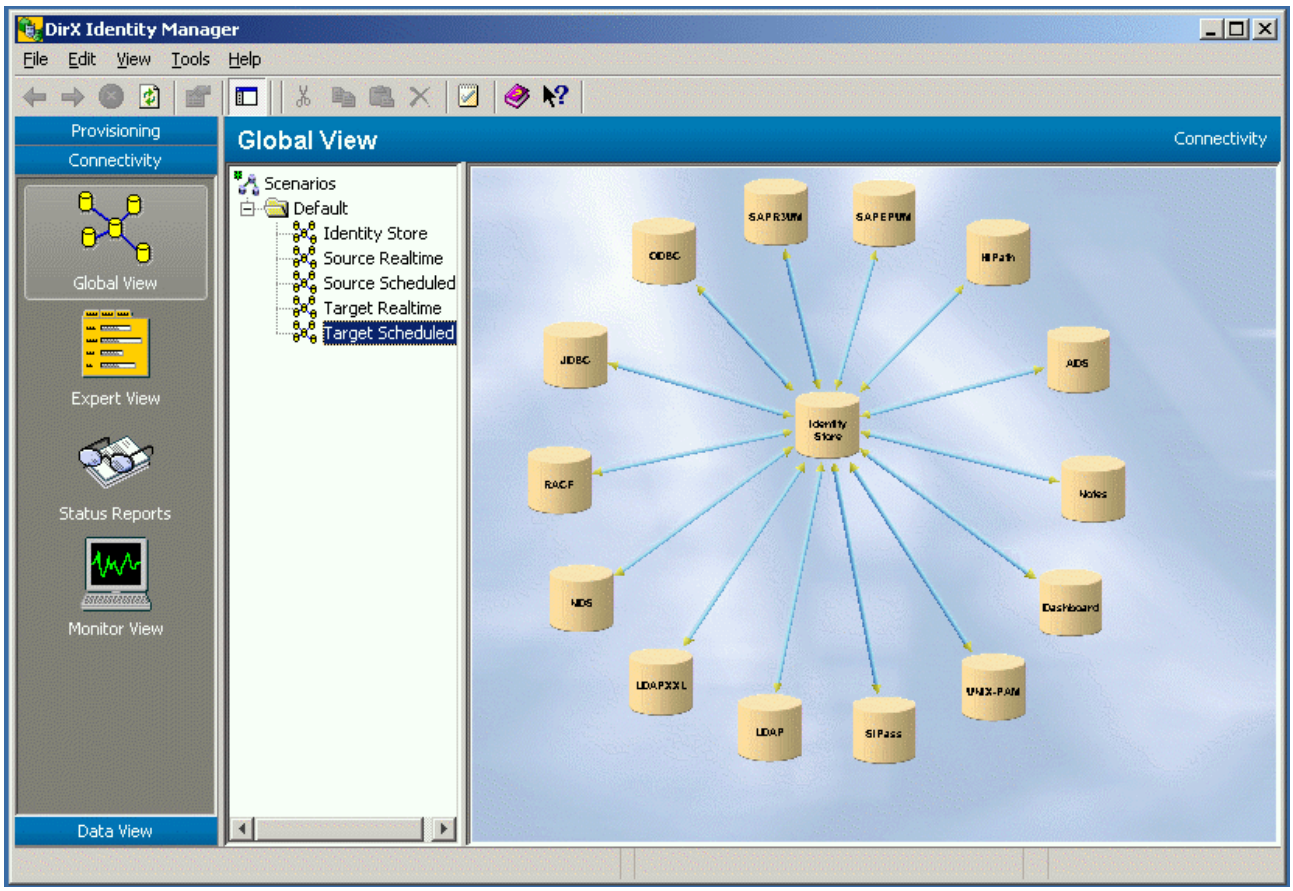

Figure 16. DirX Identity Manager Global View

The Global View shows enterprise scenarios for synchronizations between connected directories. DirX Identity Manager represents a scenario as a map of all connected directories with link lines between them for the data flow. Double-click on a connected directory icon to show its configuration in the database. Double-click on a workflow line to show the configuration dialogs for the synchronization workflow. Right-clicking on the scenario map, connected directory icons and workflow lines display context menus that allow you to perform operations on the selected items.

The next sections describe the controls available in the Global View.

3.8.1.1. Scenario Pane

The scenario pane appears in the left portion of the global view and gives you quick access to all currently existing scenarios.

The scenario pane displays the scenarios as hierarchical tree. Open the folders to find the scenario elements.

Right-click a scenario to display its context menu, which contains all the functionality from the scenario subtree in the Expert View. For more information on these selections, see "Using the Context Menu".

The most important selections on a folder are:

- **New → Folder** - Inserts a new folder at this level.

- **New → Scenario** - Inserts a new scenario leaf under the selected folder and makes it the currently active scenario (the work area displays an empty scenario map).

The most important selections on a scenario object are:

- **Rename scenario** - Renames the selected scenario object.
- **Copy Object** - Copies the selected scenario.
- **Delete scenario** - Deletes the selected scenario and the associated scenario data after requesting that you confirm the action. Note: The related workflow and connected directory information is not affected at all.

Note: If you rename a copied scenario, DirX Identity automatically renames the related folders in the Connected Directories, Jobs and Workflow folders.

Deleting a scenario only deletes the scenario map; it does not delete the related objects. To remove a scenario's objects - for example, after a Copy Scenario operation - you must delete the related folders in the Connected Directories, Jobs and Workflow folders by hand. Make sure you use the Delete operation's "check for references option" to ensure that none of the objects in these folders are linked to other scenarios.

3.8.1.2. Scenario Map

The scenario map gives you a pictorial view of the currently selected synchronization scenario. The scenario map displays connected directories as "tin" icons and displays the workflows between them as direction lines.

The scenario map background is initially blank, but you can add your company map to it.

The scenario map fills the work area completely and grows or shrinks when you resize the main window. Growing the scenario map magnifies the map and the controls placed on it. Shrinking the map shrinks the map and the controls placed on it.

Right-click in the scenario map to display its context menu. The context menu contains the following selections:

- **New Connected Directory** - Inserts a new connected directory icon. The cursor changes to a cross inside the map. Click a location in the scenario map to place the icon.
- **New Workflow Line** - The cursor changes to a cross inside the map. Click on a connected directory icon to fix the start point of the line, and then click on another connected directory icon to fix the end point of the line. This option is only available when more than one connected directory is available in the scenario.
- **Properties...** - Displays the properties of the scenario map. You can also double-click in the map to display its properties.

You can adjust the following scenario map properties:

- **Grid** - Use the Grid **X** and **Y** fields to set the grid cell width (X) and height (Y). Check or uncheck **Use grid** to switch the grid on or off.

- **Image** - Displays the file name of the background map image in use with the scenario map. Click the **...** button to select an image file from a directory. You can use any JPEG or GIF file as a background image.

Manager stores the settings you make in the scenario map properties dialog in the corresponding scenario configuration object.

Note that a scenario object only contains links to workflow and connected directory objects, which allows these objects to be shared by multiple scenarios. Changing objects shared by multiple scenarios affects the scenarios that include these objects.

3.8.1.3. Connected Directory Icon

You can place a connected directory icon at any location in the scenario map.

A connected directory icon consists of the "tin" image and a label that shows the name assigned to the icon. When you change the connected directory name (from the connected directory configuration wizard or from the connected directory configuration object in the Expert View), Manager changes the connected directory icon's label name in the scenario map.

When you resize the scenario map, the connected directory icon grows or shrinks accordingly.

Right-click a connected directory icon to display the connected directory context menu. It has the following selections.

- **Configure** - Starts the connected directory configuration wizard. If the wizard is running for the first time, it displays the list of available connected directories. Select a directory, and then use the wizard to set up your new connected directory instance.
  Note: This operation copies the selected template and creates a new connected directory object. It copies it to the Connected Directories folder into a folder that is named equal to the scenario. It does not copy channels and file objects. These are created during workflow copies. Therefore you should not create file objects in the corresponding wizard step.
- **Data Flow** - Opens the Data Flow Viewer for analyzing data flow in and out of the connected directory.
- **Open** - Performs the defined viewer command of the connected directory. Please note that each Open command in the Global View opens another instance of the viewer.
- **Move** - Enables or disables the ability to drag the icon to a different location. A flag before the menu entry indicates whether the option is enabled or not.
- **Rename** - Renames the connected directory.
- **Report** - Generates a report for selected connected directory.
- **Remove** - Deletes the connected directory icon after requesting confirmation. **Note:** the corresponding connected directory data is not deleted from the configuration database.

3.8.1.4. Workflow Line

A workflow line represents one or more synchronization workflows and is located between the center points of two connected directory icons (examples are workflows for delta or full update or for initial load). The workflow line is either unidirectional (a single arrow) or bidirectional (a double-arrow). The arrow indicates that there are one or more workflows that work in this direction.

When you resize the scenario map, the workflow lines grow or shrink accordingly.

Right-click on a workflow line to display its context menu. The menu contains the following selections:

- **New** - Starts the configuration wizard to add a new workflow to this line. If templates are not available, the wizard displays an error message. If templates are available, use the configuration wizard to configure the workflow.

Note: This operation copies the selected template and creates a new workflow object. It copies the workflow object and all activities to the Workflows folder into a sub folder that is named equal to the scenario. Additionally, it copies all related jobs, channels and file objects that belong to this workflow. The jobs are copied to the Jobs folder into a sub folder that is named equal to the scenario. The channels and file objects are created under the related connected directory objects.

- **Assign** - Links the line to an existing workflow. All templates are displayed regardless whether they fit between the two connected directories. This selection allows you to use the same workflow in different scenarios. You can then configure the same workflow from all the scenarios.
- *Workflow name* - Displays a menu for the selected workflow (*workflow name*) that contains the following items:
- **Show structure** - Starts the structure view for the workflow.
- **Configure** - Starts the configuration wizard for the workflow.
- **Run** - Starts the workflow. A "Run workflow *workflowname*" window is displayed for Tcl-based workflows (see below) or a note is displayed that the Java-based was started. Note: You can also start workflows from the Expert View or from the Target Systems view in the Provisioning view group. For more information, see the section "Using the Context Menu".
- **Remove** - Removes the selected workflow after requesting confirmation. **Note:** the workflow configuration object is not deleted from the configuration database.
- **Report** - Generates XML and HTML reports of the selected object.

3.8.1.5. Run Workflow Window

The Run Workflow window consists of two tabs:

- **General** - Shows a progress bar that indicates the status of the workflow. Above the progress bar status messages are displayed.
  Press the **Details** button to review the status messages.

During the run you can press **Abort Workflow** to stop the workflow. This aborts in any case the workflow and the actual running activities. The running agents are only aborted if the Abort Execution Allowed flag in the agent object is set (per default it is not set).
After a run, you can rerun the workflow by clicking **Run Workflow** again.

- **Structure** - This window displays the control flow of the workflow. See the **Workflow Status Structure** description in the chapter "Context Sensitive Help" in the *Connectivity Administration Guide*.

Use the **Close** button to close the run workflow window.

3.8.1.6. Using the Workflow Structure View

The structure view is a powerful tool to view and edit a workflow configuration object. The view provides a clear representation of the workflow's most important components.

Use the workflow structure view to display and edit the components that contribute to the workflow.

At the top of the view, two property items are shown:

Workflow - The workflow configuration object.

on Identity Server - The C++-based Server on which the workflow will be executed.

Below these property items is a table that contains a list of all activities that belong to the workflow ordered by their execution sequence. The table displays the following items:

Activity - The list of workflow activities, in the order in which they will run.

Identity Server - The C++-based Server on which the activity will run.

Run Object - The job to be run when its corresponding activity runs. Alternatively a workflow can be attached to this activity in case of nested workflows. In this case the rest of the columns are empty. Double-click the workflow object to open the next level of the structure view.

Channel - The input and output channels assigned to the job if Run Object is linked to a job.

Direction - The data flow direction from or to a connected directory if Run Object is linked to a job.

Connected Directory - The connected directory that corresponds to the channel if Run Object is linked to a job.

You can open more than one instance of the structure view, and the view can remain open while you are performing other tasks in the DirX Identity Manager's main window.

Click **Edit** to edit the workflow configuration object. When focusing a table cell by clicking on it or moving the focus by pressing the TAB key, the appropriate editor element appears, which can be used as described in the Expert View.

Click **Save** to store your changes. Click **Reset** to discard them. Click **Close** to close the structure view window.

3.8.2. Using the Expert View

The Expert View provides a complete view of the data in the Connectivity configuration. It is intended for use by experienced users who require access to all the configuration objects in the Connectivity configuration. The Expert View displays the logical structure of these configuration objects as a hierarchical tree and presents their properties in property dialogs. You use the tree pane to access the properties of the configuration objects in the Connectivity configuration. The following figure shows the Expert View.

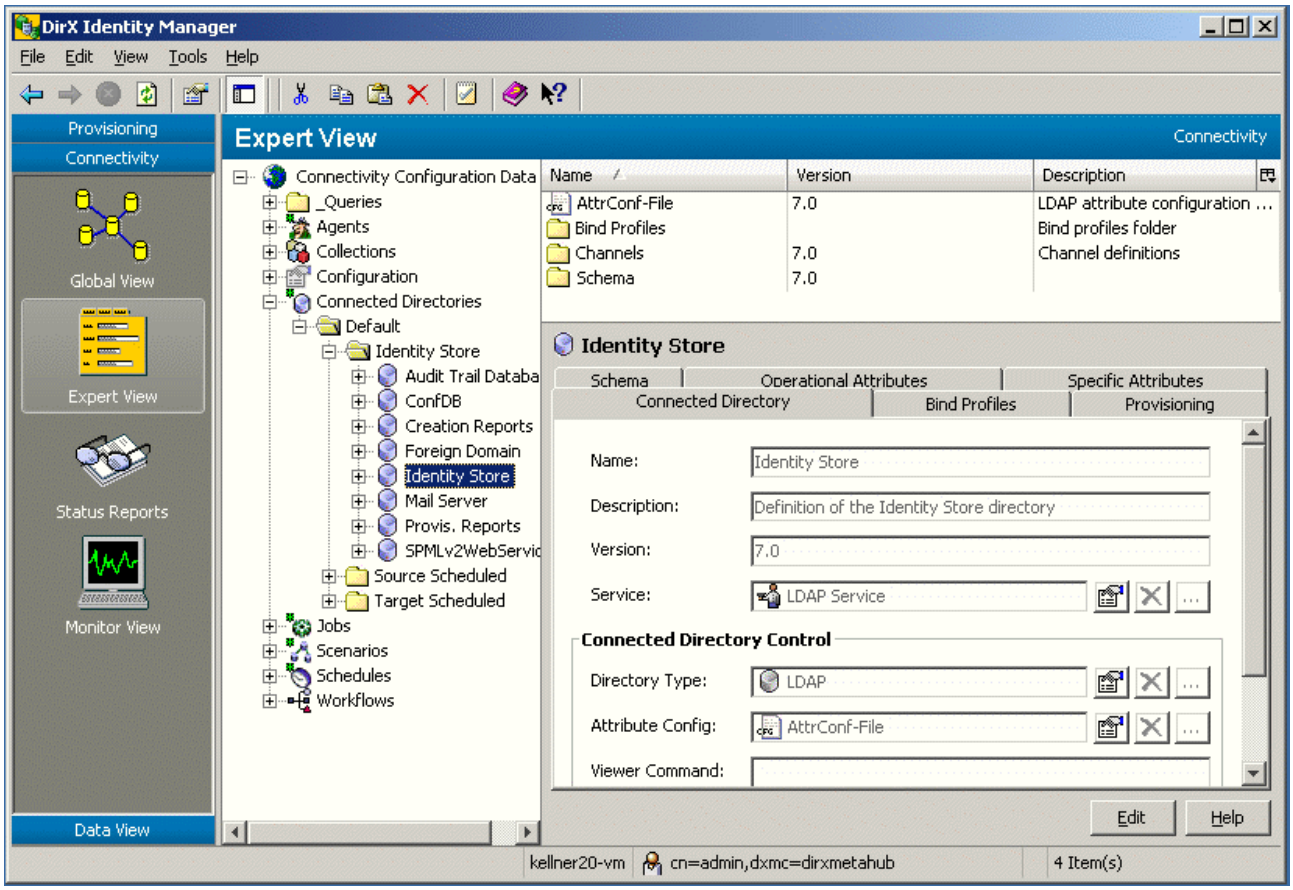

Figure 17. DirX Identity Manager Expert View

As you can see from the previous figure, the tree pane has several levels. The top-level folder represents the Connectivity configuration itself. The second level collects objects of the same type, and the third level lists the particular objects. Additional levels can also exist when they are needed.

Click **Edit** in a configuration object's property dialog to make changes to it. Most of the property items can be edited by directly typing strings into the corresponding text or number field. Other items are just yes-no alternatives and must be simply marked or unmarked. More complex items are represented by editor controls that provide buttons to open another property page or to jump to the property page of the referenced object. There are also tabular representations of value sets. These values can be modified again either by typing strings directly into the table cell or the just mentioned special editor controls are provided. Click **Save** to save your recent changes. Click **Reset** to cancel any

changes.

The next sections describe the editors that are available in the Expert View.

3.8.2.1. Using the Configuration Object Property Dialogs

When you select a configuration object in the logical tree view, the work area on the right-hand portion of the view displays a property dialog for working with the object's properties.

An object's property dialog consists of a general page that represents the object's textual, number or option properties. An object's property can also be a reference to another configuration object. For example, the service configuration object contains a system property, which is a reference to a system configuration object.

The Manager displays an object's properties in read-only mode. Click Edit to open the properties for editing. Click Save to save your changes. (You must save an object's property changes before working on another object.)

You cannot switch to another object while you are in edit mode (this is indicated by a special cursor shape when you go outside the edit window). If you click outside the edit window, Manager asks you whether you want to leave this object and save (select Yes) or not (select No) or whether you want to go back to the edit mode (select Cancel).

A property dialog in the Expert View is always based on a tabular control and can thus be composed of multiple pages that you access by tab clicks. A property dialog contains a work area that offers the following types of fields for editing the property values:

- Text fields for pure textual input
- Number fields for number input
- Fields with special input format like date, IP address etc.
- Combo and list boxes for the selection of one or more elements of a set of values
- Radio buttons for short (up to three) option lists.
- Check boxes for alternate switches
- Tables for displaying complex elements with multiple properties in tabular style

The property dialog also contains the following buttons for editing control:

- **Edit** - to switch to editing mode.
- **Help** - to open the online help that describes how to use the property dialog.

When you click **Edit**, the editing control buttons change to:

- **Save** - to save changes made since the last click on **Save**. The property dialog reverts to read-only mode and displays the new values.
- **Reset** - to discard all changes since the last click on **Save**. The property dialog reverts to read-only mode and displays the properties of the object as they were before clicking on **Edit** or **Save** respectively.

3.8.2.2. Using the Schema Displayer

The DirX Identity Manager can read the schema from any LDAP-based connected directory into the Connectivity configuration and can automatically create the attribute configuration information that the meta controller requires. You use the Schema Displayer's **Synchronize** action to direct DirX Identity Manager to read the schema of an LDAP connected directory. You can then use the Schema Displayer to view and check the read-in schema data.

Some LDAP directories - for example, Active Directory - do not allow anonymous access for a schema read. For these directories, at least one bind profile must exist for the connected directory description that can be used as the bind profile for schema read access.

Reading or updating the schema performs an automatic update of the attribute configuration information. The procedure for an update is:

- Click **Synchronize** in the schema tab in a connected directory object to read the actual schema definition from the LDAP server. Prerequisite is that the server address and the bind information are set correctly. Note that the Synchronize button does not work at the schema object level.
- When the schema read has completed, you can define all **object classes** to be transferred to the attribute configuration. Simply set the flag in the first column of the object class list.
- If you proceed to the next wizard step or click **Save**, DirX Identity asks for confirmation on whether to update the attribute configuration. If you choose **No**, no update is performed (this selection allows you to check the schema and to abort the update operation if something is not correct).
- If you choose **Yes**, the update is performed. It consists of several customizable steps:
- DirX Identity uses all object classes that are flagged in the schema object in the first column to update the attribute configuration information.
- If the flag **Include orphaned attributes** is set, then all attributes that do not belong to an object class are also used for the update operation.
- For each attribute that is not yet present in the attribute configuration, a new line is created. You can control this creation with the **Template** tab definition in the attribute configuration object (see below).
- For each modified attribute, an update is performed in the corresponding line. Manually added ';binary' suffixes are not affected by this procedure. You can control this modification with the **Template** tab definition in the attribute configuration object (see below).
- For each attribute that is no longer part of the read schema (or that is contained in an object class that is no longer flagged for update), the line is completely removed from the attribute configuration as long as the line is not flagged in the **S** column of the attribute configuration. This method allows you to define local attributes (for example, attributes that exist only in the intermediate file like ChangeType) that are not affected by the update operation.

3.8.2.2.1. Attribute Configuration Update Template

Each attribute configuration object contains a **Template** tab where you can define the update procedure. For each field in the attribute configuration line, you can define the way the update must be performed. The following options are available:

- **<?name/>** - Inserts the LDAP name of the read schema attribute into this field.
- **<?length/>** - Inserts the length of the read schema attribute into this field.
- **<?rule/>** - Inserts the match rule of the read schema attribute into this field.
- *constant* - Sets this constant string value into this field. Constant values can be mixed with <?name/>, <?length/> and <?rule/> fields.
- **=** - The equal sign as first character in a field defines that this field is updated during every schema update operation. If no equal sign is present, the field is only set during a creation of a new line. If you want an equal sign as first character in a field you must escape it with a backslash (\=).

Example: Look at the attribute configuration object of the Identity Store connected directory.

- The **Name** and **Abbreviation** fields are set to the LDAP name of the attribute (<?name/>).
- The **Prefix** field is set to the LDAP name of the attribute succeeded by an equal sign (<?name/>=)
- No **Suffix** is set.
- The **Length** field is set to the length of the LDAP attribute (=<?length/>). Because it is preceded by an equal sign, this field is also updated during a modification operation. All other fields are not touched.
- The **MV Separator** is set to the constant value ';'.
- The **Match Rule** field is set to the length of the LDAP attribute (=<?rule/>).
- The **Encryption** field is set to the constant value 'N'.

Other examples for templates you can view in the ADS, DirXdelta and NDSldap connected directory definitions.

Note: You cannot use the schema update from the Exchange, Notes, NT and RACF directories. Exchange, NT and RACF do not allow a schema read and Notes uses different attribute names for LDAP and internally (the Notes agent cannot work with LDAP attributes).

3.8.2.2.2. Accessing the Schema Displayer

In the Global View, you can access the Schema Displayer when you run the connected directory configuration wizard. In the Expert View, you access the Schema Displayer when you work on the properties of a connected directory configuration object. Both types of access are only possible if the type of the connected directory contains a schema element (which is true only for LDAP directories including ADS).

The Schema Displayer consists of two tabs:

- The Object class tab - displays the schema object classes
- The Attribute Types tab - lists all the object attributes

3.8.2.3. Using the Object Class Tab

The Object class tab shows a table that lists all object classes in the schema. The fields in the table include:

- **Name** - Contains the name of the object class. This can be any string of characters, white spaces, dashes, underlines and numbers. Other symbols (!"$%&/()=?\@+*~#',;.:<>) are not allowed
- **OID** - Holds the unique identifier for the class. This is a block of integer numbers separated by points, for example 1.3.12.2.1107.1.3.102.6.2.3.
- **Kind** - Defines the class kind of the object. The following options are available: Abstract, Auxiliary, Structural

Select an object class, and then click the details button to display the remaining class properties. This dialog contains the following fields:

- **Description** - Contains the description for the object class. This can be any text.
- **Superior class** - Contains the super-class of the respective object class. Can be empty.
- **Obsolete** - Checked if the class is obsolete (no longer used).
- **May and must attributes** - displays the same information as displayed in the Object attributes tab plus a Mandatory checkbox. If checked, the attribute is mandatory (it must have a value).

3.8.2.3.1. Using the Attributes Type Tab

The Attributes Type tab displays a list of all configured attributes. The fields shown in the table include:

- **Name** - Contains the name of the attribute. This can be any string of characters, white spaces, dashes, underlines and numbers. Other symbols (!"$%&/()=?\@+*~#',;.:) are not allowed.
- **OID** - Holds the unique identifier for the attribute. This is a block of integer numbers separated by points, for example 1.3.12.2.1107.1.3.102.6.2.3.
- **Length** - Contains the maximum length of the attribute and must be an integer. Can be empty to indicate that the maximum length of the field is undefined and can thus have any length.

The fields below the table display more details about the currently selected attribute. These fields include:

- **Description** - Contains the description of the respective attribute. This can be any text
- **Derived from** - Contains the super-class of the respective attribute and must be a valid

attribute class name

- **Syntax** - Holds the name string of the syntax rule used for the respective attribute
- **Usage** - Means the usage scope for the attribute. The following options are available: User applications, Directory operation, Distributed operation, DS operation

The "Match rules" fields include:

- **Equality** - Specifies the match rule for equality matches. The item can take one of a large set of values. Among these are the important ones: CEM (case exact match), CIM (case ignore match, OM (octet string match), DNM (distinguished name match
- **Ordering** - Specifies the match rule for ordering matches. For the value range see the comment above
- **Substring** - Specifies the match rule for ordering matches. For the value range see the comment above

The "Options" fields include:

- **Collective** - If checked, the attribute is collective (it is assigned to all objects below the defining object in the DIT)
- **Modifiable** - If checked, the attribute can be modified
- **Single value** - If checked, the attribute allows a single value only. Otherwise, it is of type 'Multi value' and can contain an unsorted list of entries.
- **Obsolete** - If checked, the attribute is obsolete (it is no longer used)

3.8.2.4. Using the Attribute Configuration Editor

The DirX Identity meta controller requires attribute configuration information for the connected directories it is to manage. This information can also be used in DirX Identity to provide information for Identity agent configuration files (*.ini files), for example, the ODBC agents.

The C++-based Server can automatically derive the necessary attribute configuration information from the schemas of LDAP connected directories that have been read into the configuration database (as described in the topic "Using the Schema Displayer"). For all other types of connected directories, the attribute configuration information must be present in the configuration database.

You use the Attribute Configuration Editor to supply the necessary attribute configuration information for a connected directory. You can use the Attribute Configuration Editor to:

- enter the attribute configuration information for a connected directory by hand into the Connectivity configuration
- import the attribute configuration information contained in an attribute configuration file (***.cfg**) into the configuration database
- Update the attribute configuration information by synchronizing the schema.

You can also use the Attribute Configuration Editor to export attribute configuration

information into a file in the file system.

In the Global View, you access the attribute configuration editor when you run the connected directory configuration wizard. In the Expert View, you access the Attribute Configuration Editor when you work on the properties of a connected directory configuration object.

The Attribute Configuration Editor displays two tabs:

- The Attribute List tab - use to enter attribute definitions for each connected directory attribute
- The Global Info tab - use to enter optional global information fields for parsing directory data files

Click **Edit** to begin entering information into the attribute list table or the global information fields.

Click **Save** to save your attribute configuration information. Please note that large schemas or attribute configurations take time to be stored in the configuration database (up to 1 minute for 1000 rows).

Click **Reset** to cancel any changes since the last save operation.

3.8.2.4.1. Using the Attribute List Tab

Each attribute in an attribute configuration has a set of attribute definition fields associated with it. Use the attribute list tab to enter the attribute definitions for each connected directory attribute. The attribute list is a table of rows and columns. Each row provides the attribute definition for one attribute. Each column in the row consists of an attribute definition field. Attribute definition fields include the attribute's:

- Name
- Abbreviation
- Prefix
- Suffix
- Encryption
- Length
- Multi-value separator
- Matching rule

See the chapter "Attribute Configuration File Format" in the *DirX Identity Meta Controller Reference* for more details about these attribute definition fields.

Use the **TAB** or arrow keys to move between the fields in the table.

Some attribute definition columns provide a pull-down list from which you can select a value. Click the down-arrow to the right of the column to display the list; click on a value to select it.

Click a row to select it. Click the **Add Row** button to add a new row after a selected row. Click the **Delete** button to delete a selected row.

3.8.2.4.2. Using the Global Info Tab

The global information portion of attribute configuration provides information for parsing connected directory data files. Use the Global Info tab to enter any global attribute configuration information required for the connected directory. Global information is optional, and can include:

- record and field separators
- continuation line and comment indicators
- object (directory entry) and attribute operation code names for LDIF-formatted files.

See the chapter "Attribute Configuration File Format" in the *DirX Identity Meta Controller Reference* for more details about the global information fields.

Each field in the Global Info tab corresponds to a global information item. Each field provides a pull-down list from which you can select a value. Click the down-arrow to the right of the field to display the list. Click on a value to select it.

3.8.2.4.3. Using Import and Export

To import an attribute configuration file into the configuration database:

1. Click **Import CFG File**.
2. From the **Import File** dialog, select the target attribute configuration file, and then click **Open**. This action reads the contents of the attribute configuration file into the Attribute List and Global Info tabs.
3. Click **Save** or **Reset** to either save or abort the operation.

To export attribute configuration information into a file:

4. Click **Export CFG File**.
5. From the **Export File** dialog, select the target subdirectory for the file, enter the file name, and then click **Save**. This action reads the contents of the attribute configuration file displayed in the Attribute List and Global Info tabs into the specified file.

3.8.2.5. Using the Selected Attributes Editor

An important step in setting up a synchronization scenario is to define the set of attributes to be synchronized between the source and target connected directories. The set of attributes to be synchronized is a subset of the total set of attributes defined in the connected directory schema.

You use the selected attribute editor to select the set of attributes to be synchronized. In the Global View, you access the selected attribute editor when you run the workflow configuration wizard. In the Expert View, you access the selected attribute editor when you work on the properties of a channel configuration object.

The selected attribute editor consists of two tables:

- Attributes in attribute configuration-displays the attributes in the connected directory attribute configuration
- Selected attributes-displays the attributes that have been selected for synchronization and any synchronization flags set for the attributes

You select the attributes for synchronization by copying them from the Attributes in the schema list to the Selected attributes list. Click **Edit** to start working with the tables.

To copy an attribute from the Attributes in the attribute configuration list to the Selected attributes list, click the attribute in the schema list to select it, and then click the **>** arrow button.

Click the **>>** arrow button to copy all the attributes from the Attributes in schema list to the Selected attributes list.

To remove an attribute from the Selected attributes list, click the attribute in the list, and then click the **<** arrow button. Click the **<<** arrow button to remove all the attributes from the Selected attributes list.

When an entry in the table on the right side is displayed with a different background color, this means that this attribute is no longer in the table on the left side. Either edit the source (the attribute configuration) or remove the attribute from the list by moving it to the left side.

To work with the synchronization flags available for the attribute:

1. In the **Flags** column, click **...** The Synchronization Flags dialog is displayed.
2. Check or uncheck a synchronization flag checkbox to enable or disable the flag. The meaning of the flags is as follows::*
   Don't add attribute* - Do not create an attribute in the target directory even if the corresponding attribute in the source directory exists. If metacp is processing an LDIF change entry, and it encounters a changetype "modify" operation with an "add" modification for a specific attribute, metacp uses this flag to verify whether it can create the attribute. In this case, the directory server may already hold the attribute; if it does, metacp creates an additional attribute value for the attribute.*
   Don't add attribute value* - Do not add additional attribute values in the source directory to the attribute in the target directory.*
   Don't delete attribute* - Do not delete the attribute in the target directory even if the corresponding attribute in the source directory is deleted.*
   Don't delete attribute value* - Do not delete a recurring attribute value in the target directory even if the corresponding attribute in the source directory does not have the recurring value.*
   Don't modify attribute* - Do not modify the attribute value(s) of the attribute in the target directory. If this flag is set, no modification at all is performed (new attribute values cannot be created, and existing values cannot be removed).*
   Replace all* - Replace the existing attribute value(s) in the target directory with the attribute value(s) in the source directory. If the directory server has no equality

matching rule for an attribute, this flag needs to be set for the attribute in order to permit it to be updated. An example of an attribute for which the directory server has no matching rule is Facsimile-Telephone-Number. The Mrule field in the attribute configuration file specifies whether a matching rule is defined for the attribute.

Hint: If you want to set an attribute initially but prohibit subsequent modification, set the flags **Don't add attribute value**, **Don't delete attribute** and **Don't delete attribute value**. You cannot use Don't modify attribute as stated above.

3. Click **Close**.

By default, the target selected attributes list is sorted. For special purposes (for example to define the field sequence in a CSV file) you can switch off the automatic sort mechanism and order the attributes to your requirements.

- Be sure you have activated the Edit mode.
- Click the right mouse button over the right table of the selected attribute editor. A context menu is displayed. Unselect the option **Sort by names**.
- Now you can shift the fields around by simply dragging them.

Click **Save** to save your changes (or click **Reset** to cancel them).

3.8.2.6. Using the Mapping Editor

The Mapping Editor allows you to edit attribute mappings for Tcl mapping files in the DirX Identity Manager. Its main features are:

- Clear representation of the mapping items by a mapping table.
- Attributes to be mapped into another can be selected from a combo-box or entered directly into the table.
- Functions are automatically inserted with the correct count of input arguments.
- Extra parameter insert for functions with variable input argument count by a simple mouse click.
- Tcl editor windows to add code to be executed before and after mapping; see the Tcl editor topic for information on how to use it.
- A Tcl editor window to add extra mapping functions after the joined entry is available during an import operation.
- Automatic generation of the appropriate Tcl code during save operations. Generated code can be checked by switching to the Tcl content viewer.

The Mapping Editor consists of two tabs:

- The mapping items tab
- The contents tab

3.8.2.6.1. What is an Attribute Mapping?

When two connected directories are synchronized by data exchange, for each entry (record) a set of attributes on the source site is converted into a set of attributes on the target site. The rule for how to convert these attributes is described and implemented in a mapping function. Each mapping function may take one or more **ingoing** (source) attributes and produces one **outgoing** (target) attribute. The ingoing attributes are called input arguments, the outgoing attribute is called the output of the mapping:

$attribute_1$, $attribute_2$, $attribute_3$, text, number, ... -› mapping function -› attribute
Input arguments mapping result

3.8.2.6.2. Mapping Items Tab

This tab contains the Mapping Editor. It consists of the following fields:

- **List of input channels** - When you start the attribute mapping, the source and target directory together with their channels are already configured. This means that normally the attributes selected for the data synchronization between the two directories are already available. The list of input channels shows the input channels that are part of the synchronization job and their role names. The role names are only important when you want to add your own Tcl code for pre- or post-mapping.
- **List of output channels** - Shows the list of output channels and their role names.
- **Mapping table** - The mapping table contains the following:
- **Input arguments** column - Lists the input arguments of a mapping item, that is, all source or target attributes going into a particular mapping function. When you click a cell of this column, a combo-box button appears at the right of the cell. You can use this button to bring up a list with all source attributes. Clicking an item copies the attribute name to the cell. The attributes are shown as role *name.attribute* name.

  It is not necessary to select the desired attribute from what can be a very long list of attributes. You can also enter it directly. The cells in this column also accept pure text. If the input is an alphanumerical string without double quotation marks, this is taken is an intermediate variable. If the text is in double quotation marks or is a pure number, it is inserted together with the double quotation marks as it is.

  Attributes that do not contain a dot are treated as variables. This allows you to use intermediate variables that can be used later on.
- **Mapping function** column - Shows the name of the mapping function for each mapping item. When you click a cell of this column, a combo-box button appears at the right of the cell. You can use this button to bring up a list of all the mapping functions that are currently available. Clicking an item inserts the function and adjusts the number of lines belonging to this mapping item according the count of input arguments.
  A description of the existing mapping functions can be found in the section "Using the Mapping Functions".
- **Output** column - Shows the resulting attributes of the mapping items. When you click a cell of this column, a combo-box button appears at the right of the cell. You can use this button to bring up a list of all target attributes. Clicking an item copies the attribute

name to all cells belonging to this item and shows them as a single cell.

Also in this column it is not necessary to select the desired attribute from the attribute list. You can enter the name directly. However, in contrast to the "Input arguments" column, double-quoted text and pure numbers are not allowed for input.

Attributes that do not contain a dot are treated as variables. This allows you to set intermediate variables that can be used later on.

Note: When an entry in the input or results column of the table is displayed with a different background color, this means that the according attribute is currently not in the source or target selected attributes list. The synchronization procedure definitely won't work! To correct this, add the missing attribute(s) to the respective selected attributes list.*
Note:* Inconsistent mapping entries may also be marked with the prefix "inconsistent." Select another item form the list if this occurs.

- **Buttons** - The mapping table contains the following buttons on the right:

	**Inserts a new empty row behind the current row.**
	Inserts a new row to add another input argument.
	Deletes a currently selected empty row or the corresponding whole mapping item.
	Deletes a single row to remove the input argument contained in this row.
	Copies table to file and opens editor.

- **Premapping** - a Tcl editor. You can use it to add code that is later inserted into the script above the mapping items and will be thus processed before mapping. Use **New Window** from the popup menu to open a large window for editing. Use the window's close button or the **Close** command from the popup menu to return.
- **Postmapping** - also a Tcl editor. You can use it to add code that is later inserted into the script below the mapping items and will be thus processed after mapping. Use **New Window** from the popup menu to open a large window for editing. Use the window's close button or the **Close** command from the popup menu to return.
- **PostJoinMapping** - a Tcl editor that presents the post join mapping code. Prerequisite is that the job already contains a Tcl script with the Anchor value set to **PostJoinMapping**. Use this script to define actions after the join operation that are dependent on the content of the joined entry. This button is only active when a script with the Anchor=PostJoinMapping is defined at the relevant job object.

3.8.2.6.3. Content Tab

This tab contains a viewer for the generated Tcl script. This is a Tcl editor window in read-only mode. Editing this Tcl script would not make sense because the next generation based on a change in the mapping editor window would overwrite this script completely.

3.8.2.6.4. Adding Your Own Tcl Scripts

If you want to write your own mapping Tcl scripts or use existing ones:

1. Select the job object where you want to create your mapping Tcl script.
2. Select **New** and then **Tcl Script** (not Mapping Script - this would create a Mapping Editor object again) from the context menu.
3. Set the **Name** and **Description** fields
4. Set the **Anchor** to **PostJoinMapping** if the Tcl script shall be used for the post join mapping. In this case it makes sense to copy the default routines from the **PostJoinMapping_default** Tcl script (see the Configuration → Tcl → Default folder).
5. Switch to the **Content** tab. Now you can either import an existing mapping script (button **Import Tcl Code...**) or write your own Tcl code with the Tcl editor.
6. Click the **File Item** tab and set the file name the mapping script will have in the work area and all the other parameters of the File Item. See the "Context Sensitive Help" chapter in the *DirX Identity Connectivity Administration Guide* or the DirX Identity Manager online help for details about a File Item.
7. Click OK to store the new object.

Next, link this object to your job object:

1. Click the job object.
2. Click the **Tcl Scripts** tab and click **Edit**.
3. Click the last button behind the line **Mapping** and select the object you have just created before in the object browser. This links your Tcl mapping script to your job.
4. If there is a **Mapping Script** object beneath your job then you can delete it now.

Note: Central use of mapping scripts is only possible for Tcl Mapping Scripts. Table based mapping scripts must be located directly under the job object and cannot be centralized or reused by other jobs!

3.8.2.7. Using the Mapping Functions

DirX Identity is delivered with several predefined mapping functions. You can find the definition of these functions in the folder **Configuration** → **Tcl** → **Mapping Functions**.

As lots of different functions exist; a naming scheme has been created so that the classification and look-up of functions can be easily done.

- Most of the functions work on **complete Tcl-Lists** (they work on all elements of the Tcl list) and therefore return a Tcl-list as the result. These functions all start with '**l**' (for example, lStringEscape).
- Routines exist that accept **single-valued Tcl list only**. These functions also start with '**l**' (for example lDNcreate). If a Tcl list at the interface is multivalued, an error will be generated. If a Tcl list at the interface is empty, an error is generated, too.
- Other functions work on **single strings** only, and therefore just return a single string. They do not start with '**l**'.

The name consists of the following parts

- A specifier that indicates whether the function delivers a list or a string (**l** for lists, nothing for non-lists)
- An ***object*** specification (for example, **String, List, Word, Bool, ...**).
- A ***function*** name (for example, **Create, Replace, Escape, ...**)
- In some cases a second ***object*** can follow.

Note: If native Tcl functions are used, the original name is used, which may not conform in some cases to the naming rules just described.

Examples:

lStringEscape - takes a list and escapes all list elements.

lBool2Integer - converts a list of boolean values to a list of integer values.

StringAppend - appends strings to build a composed string as result.

The next sections describe the functions that are available (this is a selection of native Tcl functions that make sense in the mapping editor environment and newly written functions). See the "Mapping Functions" chapter in the *DirX Identity Connectivity Administration Guide* or the DirX Identity Manager online help for a description of all Tcl Mapping Functions.

3.8.2.7.1. Agent-Specific Functions

hdmsCmd2dmsid - extracts DMS Identifier from CMD field of an HDMS record.

hdmsdata2dn - Computes a Directory distinguished name from hdms data.

hdmsData2telno - Utility to get telephone or facsimile telephone number as concatenation of HDMS Attributes.

3.8.2.7.2. Simple Comparison Functions

ifEqual - checks a variables value and sets the result to one of two values.

ifNotEqual - checks a variables value and sets the result to one of two values

3.8.2.7.3. LDIF Change Functions

addAttributes - creates an ADD attribute definition for an LDIF change file.

deleteAttributes - creates a DELETE attribute definition for an LDIF change file.

replaceAttributes - creates a REPLACE attribute definition for an LDIF change file.

3.8.2.7.4. List Functions

concat - joins lists together with a space in between (native Tcl function)

lADSpathCreate - creates an ADS path

lDNsplit - Splits a DN into the elements of a Tcl array

lBaseDNreplace - replaces the base DN in a DN

lDNcreate - creates a distinguished name (DN)

lListAppend - appends elements to a list

lListFirst - results in the first list element

lListLast - results in the last list element

lListNth - returns the nth list element

lListRest - returns the rest of the list besides the first element

lrange - returns one or more adjacent elements from a list (native Tcl function)

lreplace - replace elements in a list with new elements (native Tcl function)

lsort - sort the elements of a list (native Tcl function)

lStringAppend - appends strings to all elements of a list

lStringCompose - composes an output string from a variable number of input strings.

lStringConvertChars - replaces UTF-8 characters by underlying vowels

lStringEscape - escapes the characters **;{}** in all elements of the list

lStringEscapeLDIF - converts elements of an LDIF content file or LDIF change file

lStringEscapeVar - escapes the defined characters in all elements of the list

lStringModify - replaces either 'n' or all occurrences of string A to string B in all elements of a list

lStringPrefix - adds a string before each element of a Tcl list

lStringRange - returns all the characters of each element in the list in the range from first to last

lStringTrim - drops leading and trailing characters from all elements of a list

lStringTrimLeft - drops leading characters from all elements of a list

lStringTrimRight - drops trailing characters from all elements of a list

lStringUnescape - unescapes the characters **;{}** in all elements of the list

lStringUnescapeVar - unescapes the defined characters in all elements of the list

lWordCapitalize - first character of a word in uppercase, rest in lowercase for all elements in the list

lWordFirst - retrieves the first word in a list for all elements of the list

lWordLast - retrieves the last word in a list for all elements of the list

lWordNth - retrieves the nth word in a list for all elements of the list

3.8.2.7.5. Conversion Functions

join - create a string by joining together list elements (native Tcl function)

lBool2Integer - converts boolean values (TRUE and FALSE) to integer values (1 and 0)

lDate2GMT - converts an list of dates into a list of GENERALIZED time strings

lInteger2Bool - converts integer values (1 and 0) to boolean values (TRUE and FALSE)

lindex - returns the nth element of a list as a string (native Tcl function)

listFirst - returns the first element of a list as a string

listLast - returns the last element of a list as a string

llist - returns a list comprised of all the input arguments (native Tcl function)

lPA2String - replaces the $ characters by carriage returns

lString2PA - replaces the carriage returns by $ characters

split - split a string into a proper Tcl list (native Tcl function)

3.8.2.7.6. String Functions

RDNescape - escapes the characters **=,+;{}** in as string

RDNunescape - unescapes the characters **=,+;{}** in a string

string first - returns the index of the first position of a searched string (native Tcl function)

string index - return the character at a defined position (native Tcl function)

string last - returns the index of the last position of a searched string (native Tcl function)

string range - returns a range of consecutive characters from a string (native Tcl function)

string replace - removes a range of consecutive characters from a string (native Tcl function)
or replaces a range of consecutive characters from a string, if a new string is provided.

string tolower - returns the string in lower case characters (native Tcl function)

string toupper - returns the string in upper case characters (native Tcl function)

string trim - returns a string with removed leading or trailing characters (native Tcl function)

string trimleft - returns a string with removed leading characters (native Tcl function)

string trimright - returns a string with removed trailing characters (native Tcl function)

StringAppend - appends strings to the given string

StringModify - returns a string where either "n" or all occurrences of string A are replaced by string B

Some functions are only available for compatibility reasons. Do not use them because they will be removed in one of the next DirX Identity versions (an automatic migration utility will be provided to perform this task):

- **convert_bool** - use lBool2Integer instead.
- **convert_PA** - use lString2PA instead.
- **convert_RDN_value** - use RDNescape instead.
- **convert_value** - use lStringUnescape instead.
- **convert_value_import** - use lStringEscape instead.

3.8.2.8. Mapping Function Examples

This section shows some typical examples of how to use the mapping functions.

3.8.2.8.1. Setting Empty Attributes

Use "set sn [**llist** ""]" to set the variable sn to an empty value. Internally a one-element list is created with the value '\0'.

For export operations, the result in an LDIF file is an attribute with an empty value:

sn:

For import operations the attribute sn is not written.

3.8.2.8.2. Ensuring Single Elements

If multi-value attributes occur in the LDAP directory, ensure that only a single element is taken to fill the output attribute (if you don’t want to transfer all multi values).

User either the function **ListFirst** or **ListLast** to extract one of the values.

3.8.2.8.3. Escaping and Unescaping Characters Correctly

If a variable can contain one of the characters ';{}' you must unescape these characters during export (use the function lStringUnescape) and escape it during import (use the function lStringEscape).

3.8.2.8.4. Composing Values

Of course you can combine attributes to another one with for example "$gn.$sn@mycompany.com". This works if both gn and sn are present. Use **lStringCompose** instead to care for empty values:

set prefix [lStringCompose "." $gn $sn]

If gn="John" and sn="Smith" the result is "John.Smith", if gn does not exist, the result is "Smith" (the dot is omitted).

3.8.2.9. Defining Your Own Mapping Functions

You can define your own mapping functions which can be used like the built-in ones. This task requires Tcl programming knowledge. Once those functions are added to the **Mapping Functions** folder in the **Configuration** branch of the **Connectivity Configuration Data** tree, they will appear in the **Mapping function** combo box that appears when you select a cell in the respective column of the mapping editor.

3.8.2.9.1. How is an Attribute Mapping Written in Tcl?

Each mapping function may take one or more **ingoing** (source) attributes and produces one **outgoing** (target) attribute:

$attribute_1$, $attribute_2$, $attribute_3$, text, number, ... -› mapping function -› attribute
Input arguments mapping result

In Tcl syntax this is written as

set attribute [mapping_function $attribute_1$ $attribute_2$ $attribute_3$ ...]

Usually, the definition and implementation of mapping_function is at the top of the mapping script and written like

proc mapping_function **args** {_
# the procedure's code comes here_
}

Also, Tcl built-in routines may be used as mapping functions. In this case, there is no definition and implementation of the used function in the mapping script.

3.8.2.9.2. How is a New Mapping Function Added?

To add a new mapping function or to modify an existing one:

Go to the **Mapping Functions** folder contained in the **TCL** subfolder of the **Configuration** branch in the **Connectivity Configuration Data** tree.

You can create additional folders here to group your mapping functions.

Right-click on the folder item and select **New > Mapping Function** from the appearing

popup menu. A dialog window opens.

Type the **Name** and a short **Description** for the new mapping function. The name must be exactly the same as it used in the procedure header (**proc** ... **args** {), otherwise the execution of subsequently generated Tcl script will fail. The name given here is used to construct the mapping statement (**set** ... [...]) in the mapping procedure.
In the field **Argument Count** define the number of arguments the function will take (at least). If the number of arguments is variable, check the **Variable Argument Count** box. This information is necessary for the mapping editor: When you select this function from the mapping function list, the Mapping Editor automatically inserts the necessary amount of rows to be filled with source attributes. If the argument count is really variable, the editor allows the user to add new rows for additional argument input. Such additional rows can however be deleted again down the amount given in **Argument Count**.

Switch to the **Content** tab sheet and enter the code for the new mapping. This step requires Tcl programming knowledge. If the new mapping function is a built-in Tcl routine like the function lindex or regsub, this step is not necessary. Leave the content page empty.

Click **OK** to save the new mapping function.

Switch to some mapping that is constructed by the Mapping Editor, then go to the Mapping function column and click into a cell of this column. Click on the combo-box button and check that the new function is contained in the mapping functions list.

3.8.2.10. Using the Code Editor

The Code Editor is a special editing tool that you can use to maintain Tcl scripts, XML object descriptions, INI files, etc.. The Code Editor consists of a text-editing window and if a Tcl script is edited, a field that can be used to select a Tcl procedure. This field allows you to adjust the text window to the beginning of a specific procedure.

The Code Editor highlights keywords of the respective programming language, comments and string items and automatically checks bracket settings. To display documentation about a Tcl keyword, double-click it. The code editor also provides the Find and Replace functions available in any standard text editor.

The main features of the Code Editor are:

- Syntax highlighting for a better readability of the displayed code
- Text search and replace function
- Multiple undo and redo actions
- Caret location notification below the text windows
- Automatic detection of block ends, where a block may be a text in braces, colons or other special character combinations
- Viewer utility for resolutions of reference blocks

Especially for Tcl editing, the following features can be used:

- Quick search for Tcl procedures within the current script by simple combo box selection

- A rename utility for Tcl procedures within the current script
- A generator for inserting Tcl and DirX Identity commands and all of their parameters

The Code Editor consists of the following elements:

- Tcl procedure selection combo box
- The main editor window
- The status bar
- A popup menu

3.8.2.10.1. Tcl Procedure Selection Combo Box

The combo box at the top of the Code Editor component is initially empty. The combo box list shows all Tcl procedures contained in the current text. A Tcl procedure is determined by the keyword **proc** at the beginning of a line (or after space or tabular indents).

When you select an item from the combo box list, the editor jumps to the header of the corresponding Tcl procedure.

3.8.2.10.2. Main Editor Window

The main editor window displays the content of the current script. Keywords, comments, and double-quoted text are displayed in different colors. The Code Editor usually appears in read-only mode (text background is greyed). Click the **Edit** button at the bottom of the display to switch to write mode.

When the focus is in the main editor window and you click the right mouse button, a popup menu appears containing all command items for text manipulation.

At any time you can open a separate editor window in a larger size. Select **New Window** from the popup menu to display this window. Use the **Close** button to close it after editing.

When you click at a keyword (it is not necessary to select the keyword) and press **F1**, the corresponding manual page will be opened in the help system.

3.8.2.10.3. Status Bar

The status bar shows the row and column position of the blinking caret. If the caret is behind a brace or any other block termination character (sequence) and there is no respective counterpart, an error message that indicates this fact is also displayed here.

3.8.2.10.4. Popup Menu

The popup menu consists of the following items:

- **New Window** - Opens an extra window to allow editing in a large window with all Tcl editor features. Use the close button of the window or the **Close** command from the popup menu to return.
- **Undo** - Undoes the last write action. When invoked again, undoes the last action before the last write action. You can repeat this action up to 32 times. This item is enabled only

if there is an action that can be undone. Note, that when you type a text fluidly, all characters typed until pausing are removed by the undo operation.

- **Redo** - Does the last write action again. This item is only enabled if there was already an edit action in the current edit session. Note, that also here all characters typed until pausing are inserted again by the redo operation, if the text was typed fluidly.
- **Cut** (Ctrl-X) - This item is only enabled when a portion of text has been selected. Cuts off the selected text from the script and stores it in the clipboard. The action can either be started by clicking on this item or by pressing the keys "Ctrl" and "X" simultaneously.
- **Copy** (Ctrl-C) - The item is only enabled when a portion of text has been selected. Copies the selected text and stores it in the clipboard. The action can either be started by clicking on this item, or by pressing the keys "Ctrl" and "C" simultaneously.
- **Paste** (Ctrl-V) - This item is only enabled when the current clipboard content can be converted to text and inserted at the current position in the Tcl script. Converts the clipboard content to a text string and inserts this string at the current position of the caret. The action can either be started by clicking on this item, or by pressing the keys "Ctrl" and "V" simultaneously.
- **Find** (Ctrl-F) - This item opens the find dialog and can be used even when the document is just opened for reading. The respective action can also be invoked by pressing "Ctrl" and "F" simultaneously.
- **Replace** (Ctrl-R) - This item opens the replace dialog. The respective action can also be invoked by pressing "Ctrl" and "R" simultaneously.
- **Go to insertion point** (Ctrl-T) - This item is useful when you scrolled a long text while editing and you lost the position of your caret. Of course, it will also be made visible when you type another character. But this is sometimes not desired. This action can also be invoked by pressing "Ctrl" and "T" simultaneously.
- **Find other block end** (Ctrl-B) - This item is only enabled when the caret is currently behind a block termination character (sequence), for example an opening or closing brace etc. When invoked, the editor will show the opposite block end. The respective action can also be invoked by pressing "Ctrl" and "B" simultaneously.
- **Select all** (Ctrl-A) - Use this item to select the whole content of the currently displayed document. The action can also be invoked by pressing "Ctrl" and "A" simultaneously.

The following menu item appears when editing a Tcl script or an INI file:

- **Resolve reference blocks** - Handles reference block resolution. The item has three sub-items:

All blocks - All blocks will be resolved.*
This block only* - This item is only enabled when the caret is currently inside a reference block. When invoked, just this reference block is resolved.*
Clear reference objects* - Clears the current settings for the reference objects "workflow", "activity" and "job".

The remaining menu items appear only when editing a Tcl script:

- **Insert proc...** - Appends a new Tcl procedure to the end of the current Tcl script. Opens a prompt window to type in the name of the new procedure and inserts it as

proc *procedure name* **args {**
}

The caret is placed at the beginning of the new line behind the opening curly brace ({).

- **Rename proc...** - Renames a Tcl procedure. This item is only enabled when a Tcl procedure has been selected in the procedure-selection combo box. Opens a prompt window to type in the new name of the Tcl procedure. When confirming the new name by clicking on the **OK** button, the editor will not just exchange the header of the procedure but even more exchange the name at all appearances in the current script.
- **Delete proc** - Deletes a Tcl procedure. This item is only enabled when a Tcl procedure has been selected in the procedure-selection combo box.
- **Insert** *group* **command** - Inserts a command from one of the groups **Meta**, **Obj**, and **TCL**. The **Meta** and **Obj** groups contain all of the commands that are used in connection with the DirX Identity meta controller **metacp**. The **TCL** group contains all built-in Tcl commands. The group menu items may contain subgroups (for example, the Tcl group is divided into 4 subgroups "A-E", "F-K", "L-P", and "Q-Z"). Some command items build groups of subcommands. When you click on a particular leaf item in the menu tree, the command is inserted with placeholders for all parameters. A "|" character between items separates different options from another. See the Tcl manual pages for additional information.

3.8.2.10.5. Find/Replace dialog

When invoking the **Find**... or **Replace**... command, the Find/Replace dialog is opened. Type into the **Find what** field, what should be found. If the pattern should be matched exactly regarding the capitalization of letters, mark the check-box **Match case**. If only occurrences as isolated words should be found, mark the check-box **Whole word**. When clicking on the **Find** button, the search will start. If the caret was not at the beginning of the document, the search is done first up to the end of the text and then you are asked if you want to continue from the beginning.

The Replace dialog additionally contains a field for the replacement labeled **Replace by** and a check-box **Confirm** which is marked by default. This means that the system will request a confirmation for all matches to be replaced before doing the replacement. When clicking on the **Replace** button only the first occurrence is handled. **Replace all** will handle all occurrences instead.

3.8.2.10.6. Reference Block Resolution

The Tcl scripts and INI files may contain some special text blocks called "reference blocks". They can be resolved by using the **Resolve reference blocks** command. A special resolver module takes the source text and replaces it with the resolved one. The resolved text can only be selected as a whole and the caret cannot be placed in it. When something is currently resolved, the menu item switches to **Unresolve blocks**.

The reference blocks used in the Tcl scripts and INI files require a workflow, an activity and a job object to calculate the resolution result. In many cases, these objects are determined from the navigation history the user created when clicking on the respective items either in the Expert or Global View. For example, when you right-click a workflow line in the Global

View, then select a workflow from the popup menu and invoke the workflow explorer window by **Show structure...**, you can click **Edit** and then edit some job. If you then go from there to a Tcl script, the reference objects are already determined and you can resolve blocks (if any) without additional work. However, if you go to the Expert View, click on **Configuration** in the tree and afterwards on Tcl and select the **ControlScript** from Default, the invocation of **Resolve reference blocks** (one or all) will result in the appearance of a browser window where first a workflow must be selected followed by a second dialog where an activity must be chosen. The job is detected automatically because an activity can have only one job.

3.8.2.11. Using the Superior Info Editor

The Superior Info Editor consists of a table with three columns:

Naming attribute - Here you can define the naming attribute the following definitions belong to.

Mandatory attribute - Set the mandatory attribute name that is necessary to create the naming attribute.

Default value - Define the default value for the mandatory attribute.

For naming attributes with several mandatory attributes you have to define a separate line for each mandatory attribute.

Example:

You need to create entries under higher level nodes c, o and ou. Therefore, you should define:

Naming attribute Mandatory attribute Default value
c objectclass country;top
o objectclass organization;top
ou objectclass organizationalUnit;top

Creation of the entry **cn=Smith Joe,ou=Marketing,o=My-Company,c=DE** would then result in the creation of the c=DE, o=My-Company and ou=Marketing node if not yet present.

3.8.2.12. Using the Specific Attributes Editor

Some objects can be extended by additional attributes. There are two levels of extension:

- You can define these attributes by using the Specific Attributes Editor.
- You can describe the representation of these new attributes in XML and fill the attributes afterwards (see Virtual Object Extensions).

The objects **Configuration, Channel, Connected Directory, Job and Workflow** contain a **Specific Attributes** tab that allows you to add, modify and delete attributes:

- Click **Edit** to modify the table content.
- **Add** a new attribute by inserting a new line into the table with the first icon right to the

table. Enter the name of the attribute in the first column and the value into the second column.

- **Modify** an attribute by changing the name and / or the value.
- **Delete** an attribute by pushing the middle button right to the table.
- Click **Save** to store your results or click **Reset** to abort the edit operation.

These attributes can be used to create specific information to be used in workflows. Use references to transfer the attribute values to command lines or configuration files.

Examples:

- Parameters at a **Connected Directory** can be used to control all workflows that import and export information to this directory (for example the base node for some or all workflows).
- You can use parameters at the **Workflow** object to control the behavior of a specific workflow (for example to control several activities of this workflow with the same parameter).
- Additional parameters at a **Job** object can reflect the specific behavior of an agent. This is especially useful for scriptable agents like metacp. These scripts often require additional parameters that shall be visible at the user interface level.
- Parameters at a **Channel** object can be used to influence the workflow at this point.

3.8.3. Using the Status Reports View

The Status Reports view displays all the status reports that are configured for the Connectivity configuration. The Status Reports view shows an object tree with the default status reports and allows you to copy and create your own status reports. Reports are based on XSL Transformations (XSLT) technology. The following figure shows the Status Reports view.

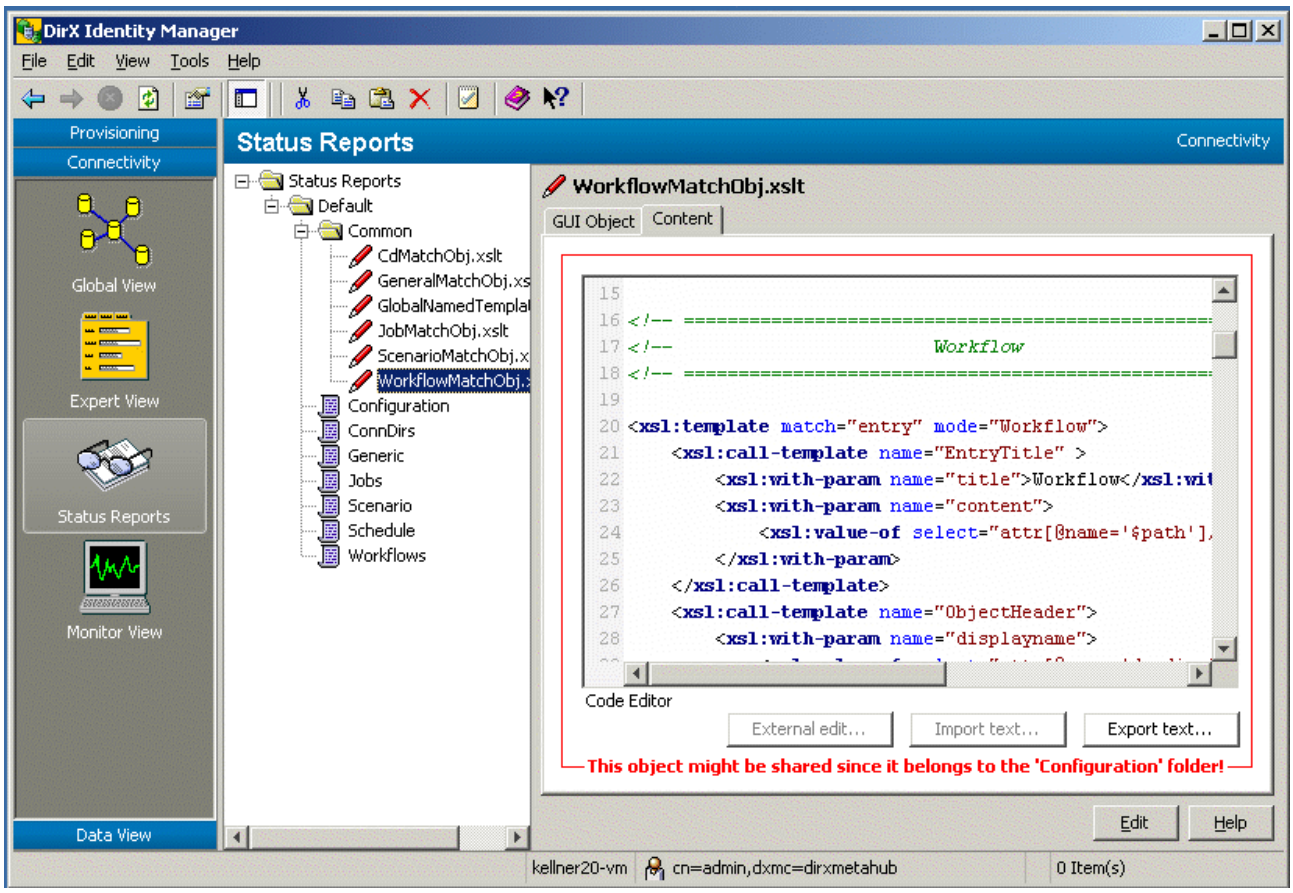

Figure 18. Status Reports View

3.8.4. Using the Monitor View

You can use the Monitor View to check the status of running and completed workflows. The Monitor View allows you to:

- Display running or completed workflows and activities.
- Display the details of running and completed workflows and activities.
- View the configuration, data, report, trace and log files created during workflow and activity operation in a fully transparent way in your whole DirX Identity domain.
- Delete workflow status entries.

The Monitor View sorts all displayed lists in alphabetical order and writes all dates in a unified format starting with the year; for example, 20001022152308Z.

The Monitor View enables you to supervise the status of all workflows in any scenario.

The left side of the Monitor View shows at the topmost level folders for each workflow that contain the results of the individual workflow runs as entries in the folder. The deepest level shows the results of the activities contained in the workflow (only for Tcl-based workflows). You can also define your own query folders to filter the results as you require (for example, to contain only erroneous runs or the workflow from the last hour).

The right side of the screen shows a list of all activities of the currently selected workflow in the tree (only for Tcl-based workflows). Below that list, the status properties of the currently

highlighted activity are shown.

The process table is a special control that contains an entry for each C++-based Server belonging to the DirX Identity domain. If you enable monitoring for a server, all running Tcl-based workflows are immediately displayed under this entry.

The structure tab of a workflow entry shows the activity structure of a Tcl-based workflow and the results in color. See the following figure.

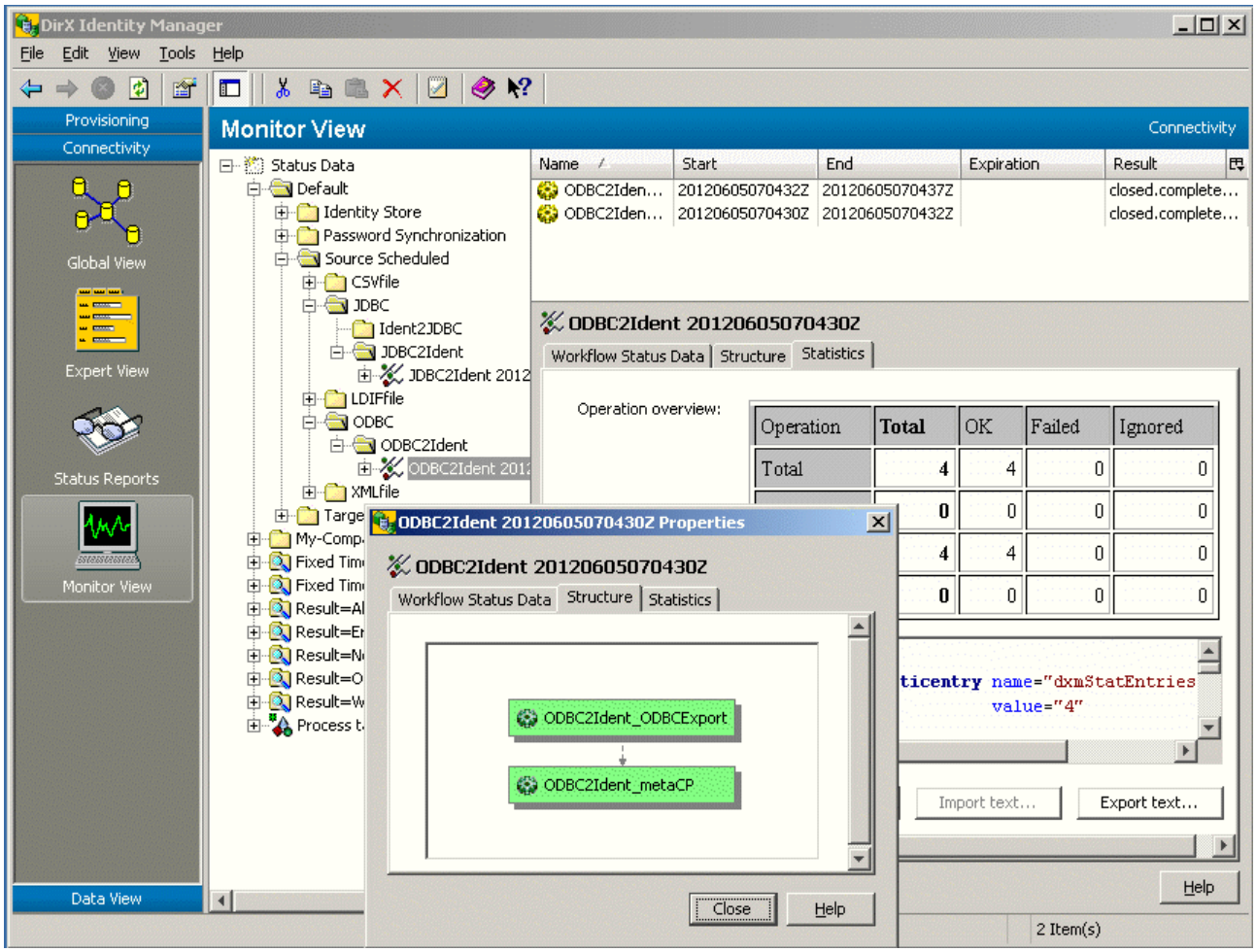

Figure 19. DirX Identity Manager Monitor View

3.8.4.1. Using the Tree Pane

The tree pane (the left-hand pane) displays a hierarchical tree of status entries. At the top of the tree is the Status Data folder. It contains hierarchical workflow folder structures, filter folders and the process table.

Opening a workflow folder structure displays the workflow status entries ordered by workflow name and date at the lowest level. When you expand a workflow status entry, the tree pane shows its activity status entries. DirX Identity automatically creates workflow folders when it runs a workflow. The created structure is equal to the structure under the Workflows folder in the Expert View.

You can create query folders to define your individual view of the status entries. Some initial folders are delivered with DirX Identity.

The **Process Table** entry contains an entry for each C++-based Server. You can enable monitoring to view running workflows in the entire DirX Identity domain but separately for each server instance.

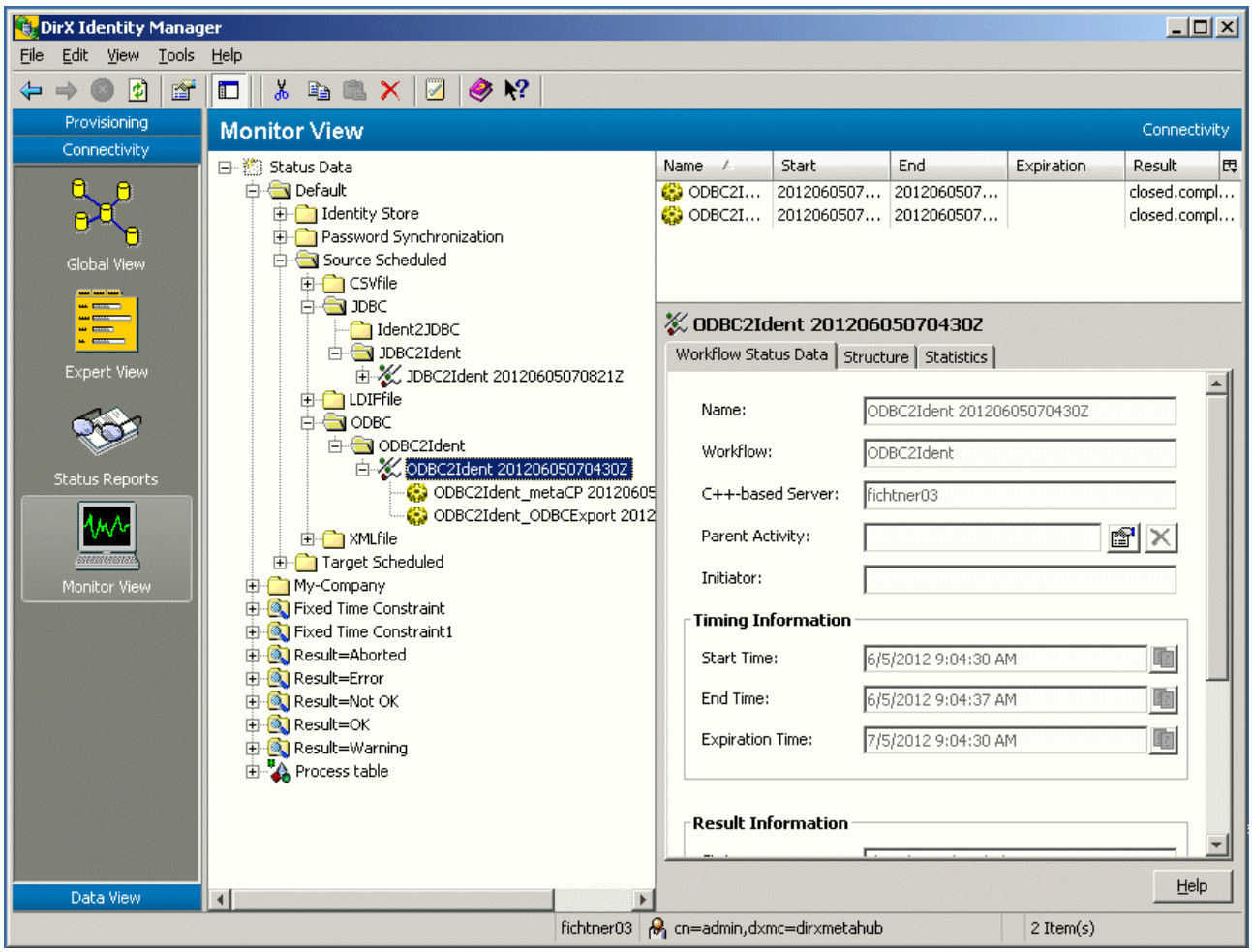

Figure 20. Monitor View - Tree Pane

Open one of the folders in the tree pane to list the next level of information in the list pane (the upper right-hand pane). Use the **Result** column to find relevant entries.

Click a workflow status entry in the tree pane to list its activity status entries in the list pane and display its properties in the object pane.

Click an activity status entry in the tree pane to display its properties in the object pane.

Special Error Status Entries

If DirX Identity is requested to start the same workflow twice or if any other error condition occurs, then DirX Identity will create entries of type:

Meta2LDIFfile_Full 20020128175803Z-E

The extension -E or -E*n*, where *n* represents an integer, indicates that the same workflow was requested to run at the same time multiple times. In this case, only workflow status entries with the relevant error messages are written. No activity status entries will be present.

No Status Entry Available

In some situations, the workflow fails but there is no status entry available because the workflow failed at a very early stage. Check that the C++-based Server is running correctly and also check the message server.

If these checks succeed, (for example, you can run other workflows without any problems) the setup of the workflow structure could be the problem. Check the event log or log files for messages about structure errors and correct them. This problem can occur when building nested workflows with parallel activities.

3.8.4.2. Using the List Pane

The list pane displays the main properties of workflow status entries and activity status entries in columns.

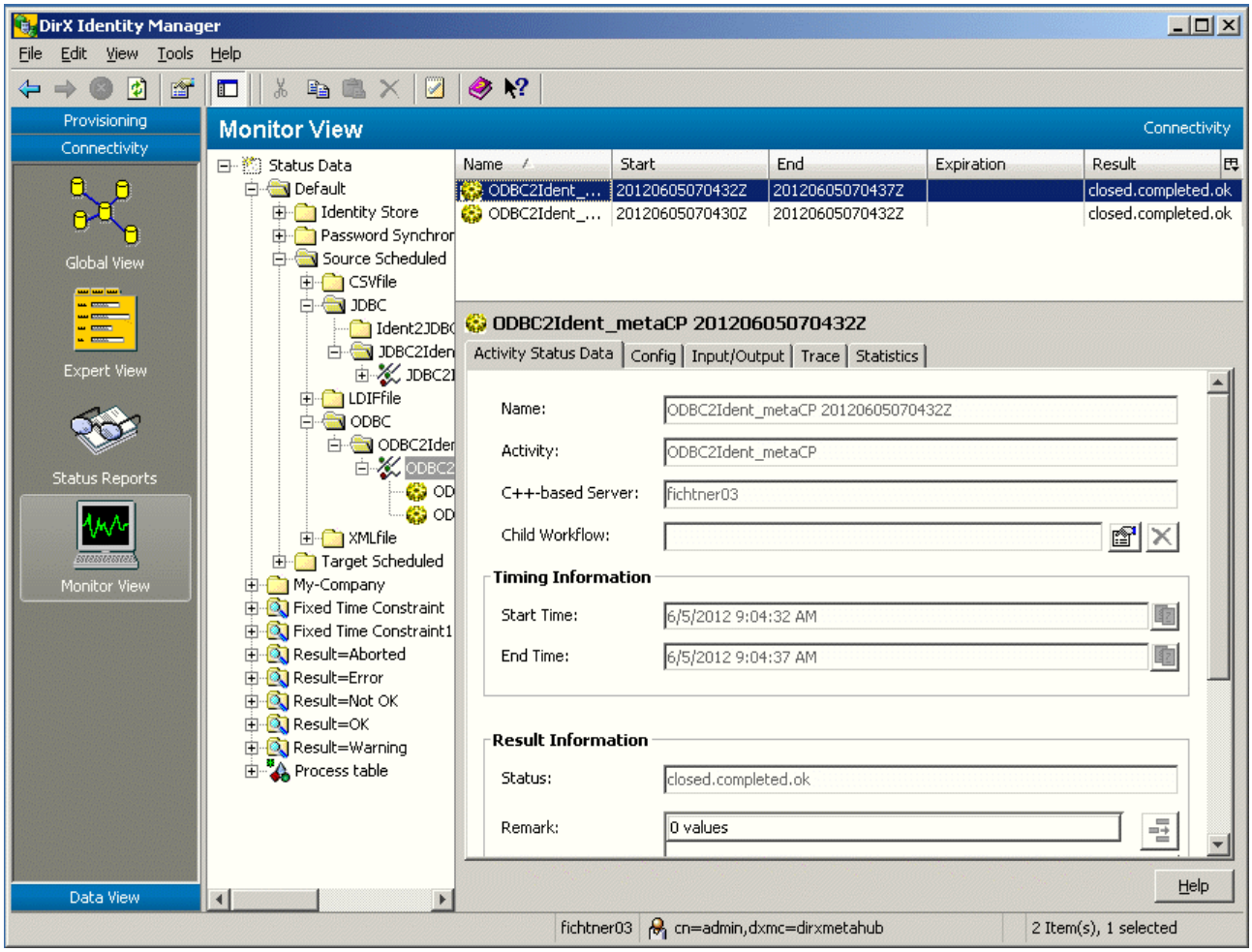

Figure 21. Monitor View - List Pane

For workflow status entries, the list pane displays:

- The name of the status entry (workflow name and date). An extension of -E or -En, where n represents an integer, indicates multiple status entries from simultaneously started workflows.
- The workflow's start time

- The workflow’s end time
- The expiration date of the workflow status entry
- The schedule that started the workflow (if you started the workflow by hand, this field is empty)
- The workflow’s name
- The workflow’s run result. See "Workflow Execution Status Values" in "Managing Provisioning Workflows" in the *DirX Identity Connectivity Administration Guide* for further details.
- The remarks (messages) that occurred during the workflow run.
- The server on which the workflow ran.

For activity status entries, the list pane displays:

- The name of the status entry (activity name and date)
- The activity’s start time
- The activity’s end time
- The expiration date of the activity status entry is always empty, because activities are deleted with the corresponding workflow entry (they "inherit" the expiration date of the workflow entry)
- The name of the activity that has generated the status data
- The activity’s run result. See "Activity Execution Status Values" in "Managing Provisioning Workflows" in the *DirX Identity Connectivity Administration Guide* for further details.
- The server on which the activity ran.
- The exit code that the agent reported.

3.8.4.3. Using the Object Pane

Use the object pane to view all the properties of a workflow or activity status entry in detail. To display a workflow or activity status entry in detail, click it in the list pane or the tree pane. The monitor view displays all the properties of the selected status entry in the object pane.

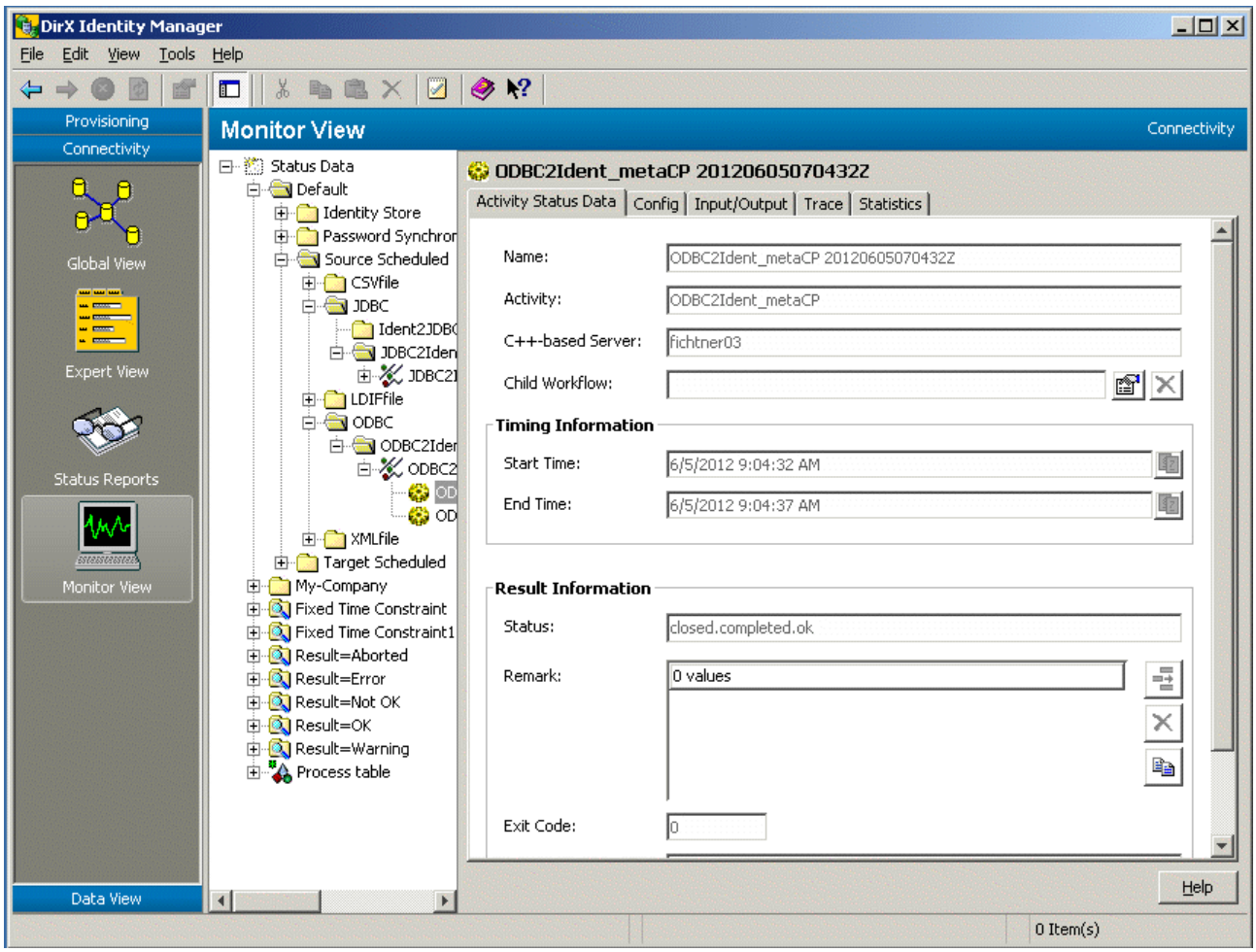

Figure 22. Monitor View - Object Pane

When you display the properties of an activity status entry in the object pane, the Files tab displays links to all the relevant files that the DirX Identity status tracker has saved in the status area. You can click the Properties button to the right of each file to display the file's content (DirX Identity Manager opens the files in read-only mode). You can configure the viewing editor that you would like to use here.

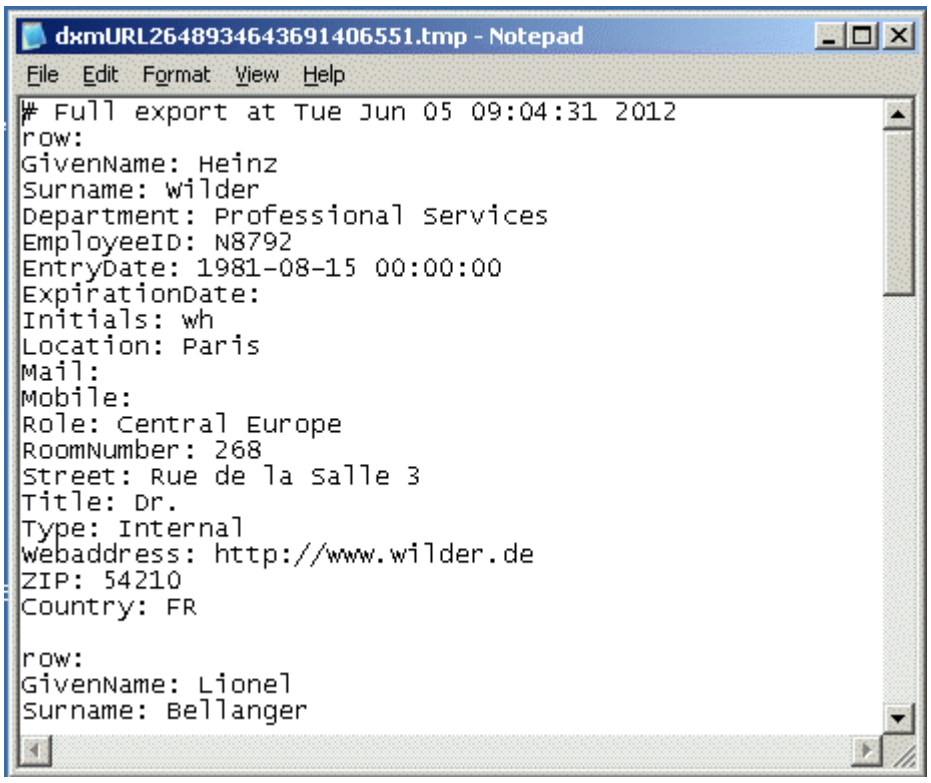

Figure 23. Monitor View - Data File Data

DirX Identity displays all workflow data even it is distributed on several physical machines. The directory entries and the stored files are some kind of hybrid database that is presented in a transparent and easy to use way.

3.8.4.4. Deleting Workflow Status Entries

DirX Identity provides two ways to handle status entry deletions (only complete workflow status entries can be deleted):

- Automatic deletion managed by an expiration timestamp
- Explicit deletion at the Monitor View.

3.8.4.5. Using Automatic Deletion

Each workflow status entry has a timestamp after which it can be deleted. The status tracker periodically scans the expiration timestamps of workflow status entries and automatically deletes the entries whose expiration time has been reached.

You can edit a workflow configuration object to adjust the value of the Status Life Time field to your requirements.

You can edit the global configuration properties to adjust:

- The values that C++-based Server uses to calculate a status file's expiration time (delta expiration time), if no value is provided in the workflow object
- The parameters that control the status tracker's automatic deletion operation (start time, interval, deviation)

To edit the global configuration properties:

1. Select the Expert View from the DirX Identity Manager main window.
2. Click the Configuration entry in the Connectivity configuration object tree. This action displays the global configuration properties.
3. Click **Edit** to edit the properties.
4. Click **Save** (or **Reset** to cancel any changes).

3.8.4.6. Using Explicit Deletion

To delete workflow status entries using the Monitor View:

1. Select the workflow status entries in the list pane.Use the **Shift** and **Ctrl** keys to select a range of entries.
2. Right-click and then select **Delete**.

You can also click on single entries in the tree view of the Monitor View and perform the same procedure.(You can't select a range of entries when you delete entries in the tree view.)

Status entries in the configuration database can have related entries in the file system status areas (see the Status Path fields in the related C++-based Server configuration objects).DirX Identity does automatically delete these corresponding directories.If necessary it uses the file transfer service to perform this task on a remote computer.

3.9. Using the Data View

The Data View contains the Connectivity and Provisioning views and displays directory data as it is stored in the directory information tree (it's a raw LDAP viewer and editor).You can use the Data View to examine and maintain the data in any directory that is accessible through LDAP.You can use the Data View to check the quality of directory entries that you have synchronized, to set the correct values to test your synchronizations, or to look up DirX Identity configuration object entries.You can also use the Data View to check the results of a synchronization workflow immediately after the workflow has finished without having to run a new tool.The following figure shows the Data View.

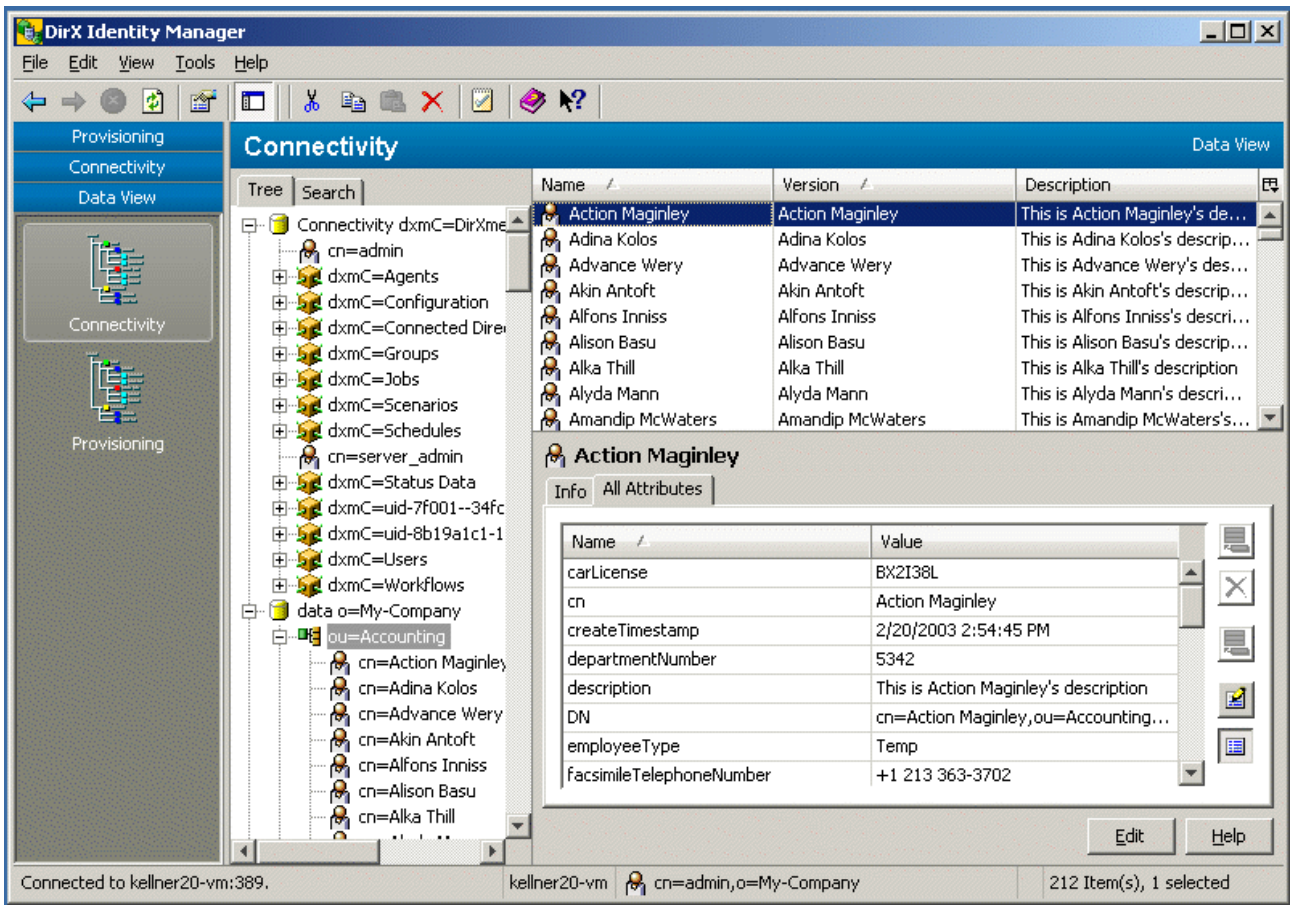

Figure 24. DirX Identity Manager Data View

The Data View displays the configuration data and the bulk data that exists in the directory.The Data View shows the directory object classes in a tree control.For each selected item, a list of attributes is displayed in the All Attributes tab as a two-column data table with attribute name and attribute value.You can also include other LDAP directories here; for more information, see the section "Customizing Server Profiles" in the section "Customizing DirX Identity Manager".

The Data View organizes the sets of data into subtrees below the root of the tree.When you click on a directory entry in the tree and you have not yet logged into the tree, the Manager prompts you to log in.The Manager then displays a property dialog that shows the directory entry's attributes.See the "Basic Patterns" topics in the "Core Components" section of the DirX Identity Manager online help for detailed information about this view.

You can use the search pane (click the Search tab) to define complex queries that allow you to view a specific set of entries.For more information on using the search pane, see the "Core Components" section of the DirX Identity Manager online help.

3.10. Customizing DirX Identity Manager

You can customize DirX Identity Manager by changing the parameters in the following files on a per-machine basis:

- dxi.cfg

- View group files
- dxmDataView.xml

3.10.1. Customizing the Property File (dxi.cfg)

The DirX Identity Manager file **dxi.cfg** is a Java property file.Each property is described by *property name=property value*.Lines can be commented with a leading #.The following table describes the supported properties.

The file is located in the path *install_path***GUI\bin\dxi.cfg**.

If you change parameters in this file, you must restart the DirX Identity Manager for the changes to take effect. If the file is not present, DirX Identity Manager uses the default values listed here.

This file also works in the home directories of other processes, which allows you to specify additional parameters for Web Services or Web Center.

The configurable parameters are:

- **aclmgr.refresh.interval** (default is 600 seconds = 10 minutes) - defines the maximum interval at which the access policy cache is refreshed or updated. A value higher than 86400 seconds (24 h) defaults to 10 minutes.
- **allow.QueryFolders** (default is **false**) - if set to **true**, the creation of query objects is allowed in the Expert View. Otherwise, this feature is disabled.
- **allow.TopLevelFolders** (default is **false**) - if set to **true**, you are allowed to create top-level folders in the Expert View. If set to **false**, you are not allowed to perform this task.
- **assign.InitialSearch** (default is **false**) - if set to **true**, privilege lists are populated with a complete initial search after clicking **Edit** in a user object. If set to **false**, the search must be performed manually.
  Note: This is a compatibility switch. For high performance, set this switch to false.
- **cache.update** (default is **timestamp**) - specifies the update interval of DirX Identity Manager's local data cache. Specify one of the following options:*
  always* - The cache is updated any time a DirX Identity object is accessed.*
  timestamp* - The cache is updated when the modification timestamp of the respective object has changed since it was last read.*
  never* - The cache is never updated. This selection means that every accessed object is just read once.
- **cache.mru.size** (default is **100**) - specifies the number of most recently used (MRU) objects that will not be removed from the cache. DirX Identity Manager prevents all objects in this list from being removed by the garbage collector.
- **cache.prefetch.size** (default is **50**) - specifies the number of objects to be read in one search operation.
- **clipboard.viewer** (default is **notepad.exe**) - specifies the clipboard viewer to be invoked when you perform the "copy" action (see Schema, Attribute Configuration, the Remarks field in the monitor view). UNIX-specific configuration lines are already contained in this file.

- **collection.base64** (default is **false**) - defines the file format for collection export.*
  TRUE* - Complex attributes of a collection are exported in base64 format. This is standard LDIF format.*
  FALSE* - Complex attributes of a collection are exported in a proprietary text format that is useful when working with configuration management systems (for example ClearCase).
- **collection.maxlinelength** (default is **0**) - allows defining the maximum length of a line when a line is wrapped during collection export. A value of zero means that no wrapping is performed at all.
- **collection.pagesize** (default is **0**) - a value greater than 0 enables paging with the specified size for internal oneLevel searches made during the export of a collection. A value of 0 means that no paging is performed.
- **design.mode** (default is **on**) - if set to **on**, the design mode feature (icon in the taskbar) is visible. Otherwise, design mode is switched off.
- **DiagPropVisible** (default is **false**) - if set to **true**, technical debug information will be added to the general property page (java-class, X500 object class, and so on).
- **export.directory** (no default) - specifies the initial path of the export file dialog box.
- **file.editor** (default is **notepad.exe $file**) - specifies the application to be invoked to display and edit ASCII files in the monitor view. The $file parameter is replaced by the respective filename. UNIX-specific configuration lines are already contained in this file.

  You can define different editors for specific file extensions. For example:
  file.editor.html=IEXPLORE.EXE "$file"
  In this case the Internet Explorer is used to view HTML files.

Note: Be sure that the editor is accessible via the defined path variable at the system level. If not, use an absolute path in your file.editor definition. This path must be defined with '/'. Backslashes on Windows platforms do not work.

Note: The UNIX-specific configuration lines assume that the variable $EDITOR is set to a path to an editor with a graphical user interface (**vi** does definitely not work!). Otherwise, the following lines do not work:
file.editor=sh -c "$EDITOR '$file'"
clipboard.viewer=sh -c "$EDITOR '$file'"

- **GenericPropertyPage.width** (default is **500**) - the initial width of property pages inside dialog boxes in pixels.
- **import.directory** (no default) - specifies the initial path of the import file dialog box.
- **ldap.filter.maxsize** (default is **100 000**) - maximum size of the search filter in an LDAP search in bytes (default 100,000).
- **ldap.maxresults** (default is **0**) - the maximum number of entries to be read during an LDAP search operation. When set to **0**, there is no limit on the client site.
- **ldap.servertimelimit** (default is **0**) - the LDAP time limit (the default is 0 which means infinite).
- **ldap.switch2offline** (default is **500**) - maximum number of DirX Identity Provisioning

objects that are to be resolved online in the DirX Identity Manager (Provisioning) session (during the privilege resolution). If this limit is exceeded, the relevant objects are flagged with the dxrTBA flag and resolved in background (you need to schedule a privilege resolution workflow). Note, that flagging many objects still needs some time!

- **ldap.trace** (default is **on**) - if set to **on**, the LDAP trace is written to the path *install_path*\Gui\logs**. If set to off, LDAP tracing is disabled. If set to filename, the LDAP trace is written to filename. Default file names are *ldap.DirXmetaRole.* ***nnn***.log* (Provisioning view) and **ldap.DirXmetahub.*nnn***.log* (Connectivity view).
- **MessageServer** - defines the message server type to be used for JMS messaging. Valid values are:*
  ATS* - DirX Messaging.
- **ModalWindow.sizeFactor** (default is **85**) - the size in % of a modal window relative to the screen size.
- **monitorview.refresh** (default is **on**) - defines whether the monitor view is refreshed when you switch to it.
- **nationalization.isRelevant.Connectivity** (default is **false**) - defines whether nationalization information is exported from the Connectivity view group.
- **nationalization.isRelevant.Provisioning** (default is **true**) - defines whether nationalization information is exported from the Provisioning view group.
- **nationalization.csv.delimiter** (default is '**;**') - lets you define the delimiter for export of nationalization information.
- **processtable.refresh** (default is 30 seconds) - the process table is regularly refreshed to show the actual state. Heavy load on the server could result in a situation where the Manager does not react anymore. If you set the switch to 0, you must perform manual refresh.
- **report.sizelimit** (default is 1000) - defines the size limit for reports.
- **resolution.mode** (default is **online**) - defines whether resolution is performed immediately (online) or in background (off-line) after you have changed a privilege that affects users. For off-line mode, you need to schedule a provisioning resolution workflow. See also the ldap.switch2offline option.
  Note: for Web Center, this flag is always set to off-line to enhance performance.
  Note: you can configure an off-line resolution for user changes via the **offlineresolution** switch at the domain object. For more information, see the *DirX Identity Provisioning Administration Guide*.
- **scheduler.sync** (default is **on**) - specifies whether a schedule modification automatically sends a synchronization request to the scheduler
- **serverstate.timeout** (default is 20 sec) - you can influence the timeout value for the Get Server State dialogue.
- **siemens.dxm.storage.beans.JnbBoolean.markemptyvalue** (default is **false**) - boolean attributes in the directory can contain the values 'true' and 'false'. If a boolean attribute does not contain a value (it is empty), the check box is surrounded with a red border if this flag is set to 'true'.
- **siemens.dxm.storage.beans.JnbStringTag.markemptyvalue** (default is **false**) - string attributes in the directory can contain any text value. If a string attribute does not

contain a value (it is empty), the display field is surrounded with a red border if this flag is set to 'true'.

- **statustracker.sync** (default is **on**) - defines whether the status tracker should delete status messages (**on**) or the DirX Identity manager itself (**off**).
- **StructureView.widthFactor** (default is **95**) - the width in % of the structure view window relative to the screen size.
- **time.display** (default is **local**) - specifies the representation of time values. Could be either **local** time or **GMT**.
- **trace.fileprefix** (default is **dximanager**) - the prefix of the trace output filename. The complete filename is structured as follows: **prefix.*nnn***.log*, where *nnn* is a number beginning with 000. The number is increased by 1 until the maximum file size **trace.maxlines** is reached. System variables like %*USERNAME*% can be used in fileprefix. Variables are replaced with their corresponding values if defined or with an empty string otherwise. See the **trace.path** parameter for the location where the file is created.
- **trace.path** (default is *install_path*\GUI\log*) – specifies the directory where the trace file will be stored. Every backslash in the path must be doubled. For example, the path **C:\\Atos\\log** is in the correct format. System variables like %*LOCALAPPDATA*% can be used in the path. Variables are replaced with their corresponding values if defined or with an empty string otherwise.
- **trace.level** (default is **1**) - trace level values are:
  0: no trace, no error!
  1: error
  2-4: warnings
  5-8: flow trace
  9: debug
  Higher levels include the content of lower levels. This means: if you specify 5, also errors and warnings are written.
- **trace.maxlines** (default is **5000**) - maximum number of messages written into one trace file. If this limit is reached, trace output switches to another file with the increased number. A value of 0 prevents switching: all messages are written into one single file.
- **trace.timestamp.format** (default: no timestamp information) - define a format string to enable time stamp information before each log entry in the trace file.
  Example:
  trace.timestamp.format=EEE MMM d HH:mm:ss.SSS yyyy
- **trace.transcript** (default is **off**) - for debugging only:*
  off* - Do not write trace messages to the console
  on - Write trace messages to the console
- **write.cache.enabled** (default is **true**) - controls whether or not modifications of target system group objects are cached until the end of an online role resolution phase.

3.10.2. Customizing View Group Files

DirX Identity Manager is delivered with two files that configure the Connectivity and Provisioning views:

*install_path***GUI\profiles\dxrViewGroup.xml** - configures the Provisioning view group.

*install_path***GUI\profiles\dxmViewGroup.xml** - configures the Connectivity view group.

This section explains how to use these files to make changes to the Connectivity and Provisioning views. All the following examples relate to the Provisioning view group. We recommend that you open the file **dxrViewGroup.xml** to help you understand the information presented here. Note that you must restart DirX Identity Manager to view the effects of configuration changes.

3.10.2.1. Understanding the File Structure

The following file defines a **viewgroup** that contains a set of **views**. The view group is displayed as a blue bar, and each view is displayed as a clickable icon.

```
<?xml version='1.0'?>
<viewgroup name="dxrManager" displayName="Provisioning"
server="DirXmetaRole" serverGroup="DirXmetaRole">
<view name="dxrUser" displayName="Users"
iconBase="siemens/dxr/manager/resources/icons/user">
<splitpanel orientation="horizontal">
    <tabbedpanel>
        <treepanel displayName="Tree" name="tree">
            <genericnode
class="siemens.dxr.manager.nodes.MetaRoleRootNode" name="cn=Users"
displayName="Users"/>
        </treepanel>
        <ldapquicksearchpanel name="search" displayName="Search"
server="DirXmetaRole" objectClasses="dxrUser"/>
    </tabbedpanel>
    <splitpanel orientation="vertical">
        <listpanel listento="tree search" hideIfEmpty="true">
            <listconfig>
                <column name="displayName" displayName="Name"/>
                <column name="description"
displayName="Description"/>
                <column name="dxrState" displayName="Status"/>
                <column name="employeeType" displayName="Emp. Type"/>
                <column name="c" displayName="Country"/>
                <column name="l" displayName="Locality"/>
                <column name="dxrTBA" displayName="TBA"/>
                <column name="dxrInconsistent"
displayName="Incons."/>
```

```
            </listconfig>
        </listpanel>
        <propertiespanel listento="tree search listpanel"/>
    </splitpanel>
</splitpanel>
</view>
    <view name="dxrBusinessObjects" displayName="Business
&#x0a;Objects"
iconBase="siemens/dxr/manager/resources/icons/directoryview">
...
</view>
   ...
    <view name="dxrDomain" displayName="Domain &#x0a;Configuration"
iconBase="siemens/dxr/manager/resources/icons/domain">
...
</view>
</viewgroup>
```

The complete file defines a Provisioning **viewgroup** that contains Users, Business Objects and other **views**. Each view can consist of a pane structure. You can define horizontal and vertical **splitpanels**. The Users view defined in the file has two horizontal panels: the first is a **tabbedpanel** and the second is a **splitpanel**.

The **tabbedpanel** consists of a tree (the **treepanel**) and a search tab (the **ldapquicksearchpanel**).

The vertical **splitpanel** consists of a **listpanel** and a **propertiespanel**.

Most of the properties of the XML elements are easy to understand. The next sections describe the important parts that you can customize, for example, to hide or add complete views and configure search panels or list panels.

3.10.2.2. Configuring Complete Views

You can easily remove a complete view if you remove the entire XML section. For example, if some of your administrators should not be able to view the **Policy** view, remove or comment this section from the file:

```
<view name="dxrPolicies" displayName="Policies"
iconBase="siemens/dxr/manager/resources/icons/policies">
<splitpanel orientation="horizontal">
...
</splitpanel>
```

```
</view>
```

3.10.2.3. Configuring Search Panels

The search panel (ldapquicksearchpanel) allows you to define the attribute lists that are visible in the **Search for** area. Configure all object classes whose attributes are to be visible, for example:

```
<ldapquicksearchpanel name="search" displayName="Search"
server="DirXmetaRole" objectClasses="dxrRole dxrPermission
dxrTargetSystemGroup"/>
```

Now you can select these object classes from the **Object class(es)** list. The names are more readable, for example dxrRole is displayed as Role, because they come from the display name attributes of the relevant object descriptions. After selecting a specific object class, all related attributes are now available for search. The attribute names are also the display names of the relevant property descriptions in the object descriptions.

3.10.2.4. Configuring List Panes

You can easily configure the columns of list panes. For example, see the Users view definition:

```
<listpanel listento="tree search" hideIfEmpty="true">
<listconfig>
 <column name="displayName" displayName="Name"/>
 <column name="description" displayName="Description"/>
 <column name="dxrState" displayName="Status"/>
 <column name="employeeType" displayName="Emp. Type"/>
 <column name="c" displayName="Country"/>
 <column name="l" displayName="Locality"/>
 <column name="dxrTBA" displayName="TBA"/>
 <column name="dxrInconsistent" displayName="Incons."/>
</listconfig>
</listpanel>
```

This definition hides the list panel completely if the selected leaf object has no more children (hifeIfEmpty="true"). The next section lists the columns. You can define the LDAP attribute name and a display name for each attribute. To guarantee a consistent user interface, the display name should be the same as the display name configured for this attribute in the properties section of the object description.

This list of attributes defines the initial state of the definitions when they are loaded for the

first time in your DirX Identity Manager instance. Now you can move columns, resize them or hide them (set or reset the flags of the context menu of the header to perform this task). You can reset everything to the initial state if you use the option **Reset to default** from the menu. You can sort all columns. All of these individual settings are stored with your Manager instance.

Warning: Using the 'More...' menu in the Search tab destroys your configuration. You must restart the Manager and perform a new search to fix this problem.

3.10.3. Customizing the Look and Feel

With version 8.2C, a new Look and Feel has been introduced for the DirX Identity Manager. A Look and Feel called classic is also available, which is mainly similar to the old Look and Feel. If you prefer the classic style, you can switch to it the following way:

- In *install_path***GUI\bin** edit the startscript **dxi_run.bat** (or .sh).
- Put the actual Java call into comments and then un-comment the one beneath the comment: "REM to enable the classic look & feel uncomment the following line and comment above line".

Snippet:

```
start "dxrManager" "%DXR_JAVA_HOME%\bin\javaw" -Xm…
REM to enable the classic look & feel uncomment the following line
and comment above line
REM
REM start "dxrManager" "%DXR_JAVA_HOME%\bin\java" -Xmx512M %jc%
%tftimestamp% -Ddirxjdiscover.lookAndFeelStyle=classic -Dswing…
```

3.10.4. Customizing Workflow Template Selection (wfwizard.cfg)

You can access this file using the path *install_path***Gui\bin\wfwizard.cfg**. This file describes the "template" step of the wizard for creating a new workflow in the Global View. The presented workflows are sorted. The sort criteria are defined via the **templatechooser.sort** property. The default

templatechooser.sort=objectclass,$displayname

specifies that the list is sorted by the attributes **objectclass** and **$displayname**. That is first the type of workflow(=objectlass) is evaluated (Tcl based - Java based workflows) and then the pseudo property **$displayname** is used for sorting.

You may define other sort criteria like **$path** (for the readable path of workflows) or other properties. Sort mode ascending is the default. For descending sort, use *propertyname*:desc*.

In the following example, **objectclass** is used as the first sort criterion and the **path** in

descending order as second sort criterion:

templatechooser.sort=objectclass,$path:desc

4. Using DirX Identity Server Admin

The DirX Identity Server Admin is a component of the High Availability suite. Use Server Admin to:

- Display the Java-based Servers, C++-based-Servers and Message Brokers with their states and other attributes
- Move adaptors from one Java-based Server to another Java-based Server
- Move the request workflow engine or the Java scheduler from one Java-based Server to another Java-based Server

The topics in this chapter provide usage information about Server Admin.

4.1. Logging In to Server Admin

To log in to Server Admin in non-SSL mode, start your browser and then enter the following URL:

http://*server*:_port_**/serverAdmin**

For example:

http://myserver:40000/serverAdmin

where **myserver** is the machine where your Java-based Server runs and **40000** is the port that you entered during initial configuration.

If you have multiple Java-based Servers running, you may use any of these IdS-J servers, for example

http://myserver2:41000/serverAdmin

If you selected SSL for the Java-based Server during configuration, use the following URL to log in securely to Server Admin:

https://*server*:_port_**/serverAdmin**

For example:

https://myserver:40443/serverAdmin

where **myserver** is the machine where your Java-based Server runs and **40443** is the port that you entered during initial configuration.

Server Admin displays a login dialog that requests a username and a password. It expects to receive your common name and your password in the LDAP data store. Only users who are members of the ServerAdmin group in the DirXmetaRole target system can successfully log in.

4.2. About the Page Layout

The default page layout consists of a header at the top, a footer at the bottom and an application-specific dialog area. All pages contain the same header, which consists of:

- A company logo and company name.
- Information about the user login status, which is either **Not logged on** or **Welcome** *username*.
- A logout link (if a user is logged on). Click this link to log out of Server Admin.

The following figure shows the Server Admin header.

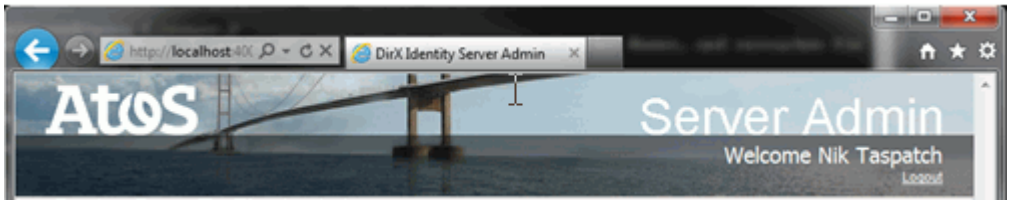

Figure 25. Server Admin Main Page Header

While Server Admin loads a new page from the server or updates the current page, an animated image is displayed in the upper left corner, as shown in the following figure:

Figure 26. Server Admin Busy Indicator

If the animation is displayed but not started, check if you have disabled playing animations in your browser.

4.3. Using the Server Overview Page

After successful login, Server Admin displays the DirX Identity Server Overview page, which is shown in the following figure:

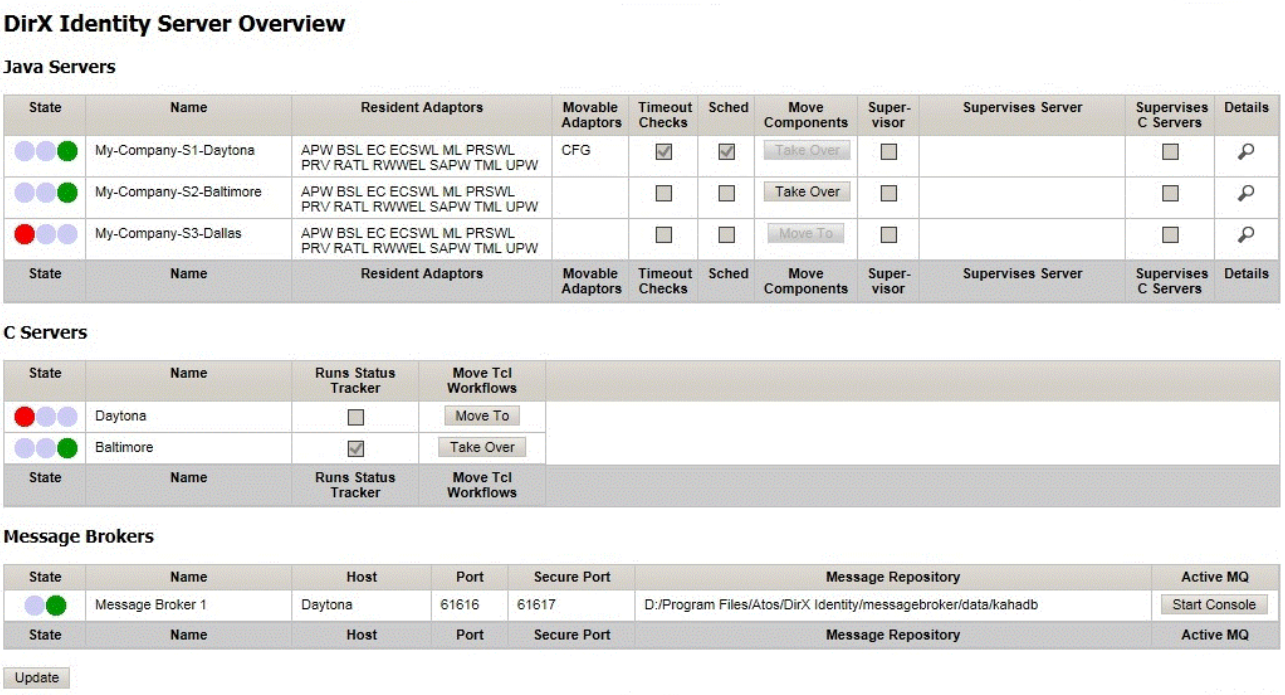

Figure 27. Server Overview Page

The Server Overview page displays tables of Java-based Servers, C++-based Servers and Message Brokers.

To update the display, click the **Update** button located below the tables.

4.3.1. Viewing Java-based Server Status

The DirX Identity Java Server table displays all Java-based servers that belong to the same domain as the server hosting Server Admin.

Each row contains status information about one server. In the figure shown in "Using the Server Overview Page", three Java-based Servers are shown. For each Java-based Server, the following information is displayed:

- **State** - the server's state, displayed as a traffic light. Possible states are:

  the server is down or is not responding.
  the server is running under heavy load (low on resources).
  the server is up and running.

- **Name** - the server's name in the Connectivity database.
- **Resident Adaptors** - the resident adaptors reside permanently on the server. They can be activated or deactivated. The field's tooltip displays the full adaptor names. (See the Details page for details.)
- **Movable Adaptors** - a movable adaptor can only run on one server of the domain. It can be moved from one server to another one. The field's tooltip displays the full adaptor names.
- **Timeout Checks** - a flag marking the Java-based Server that performs request workflow

timeout checking. This component can be moved to another server.

- **Sched** - a flag marking the Java server that hosts the Java scheduler. This component can be moved to another server.
- **Move Components** - moves an adaptor, the request workflow timeout checker, or the Java scheduler.
- **Supervisor** - whether (checked) or not (unchecked) a supervisor is running on the server.
- **Supervises Server** - the Java-based Server under supervision.
- **Supervises C Servers** - whether (checked) or not (unchecked) a supervisor is running on the server that supervises the C++-based Servers.
- **Details** - displays the server details.

4.3.2. Viewing C++-based Server Status

The DirX Identity C Servers table displays all configured C++-based Servers.

Each row contains status information about one server. In the figure shown in "Using the Server Overview Page", two C++-based Servers are shown. The following information is displayed for each server:

- **State** - the server's state, displayed as a traffic light. Possible states are:

   the server is down or is not responding.
   the server is running under heavy load (low on resources).
   the server is up and running.

- **Name** - the server's name in the Connectivity database.
- **Runs Status Tracker** - whether the status tracker runs on this server. The status tracker can be moved to another server.
- **Move Tcl Workflows** - takes over or moves all Tcl workflows being hosted by the server from/to another server or moves the status tracker to another server

4.3.3. Viewing Message Broker Status

The Message Broker table displays all configured message brokers.

Each row contains status information about one server. In the figure shown in "Using the Server Overview Page", the following information is displayed:

- **State** - the server's state, displayed as a traffic light. Possible states are:

   - the server is down or is not responding.
   - the server is up and running.

- **Name** - the server's name in the Connectivity database (also the service name on Windows).
- **Host** - the server name with the installed Message Broker.

- **Port** - the message port.
- **Secure Port** - the message port for secure communication.
- **Message repository** - the location of the database file. For more than one broker, a shared repository on a shared drive is required.
- **Active MQ** - to access the Message Broker's Web Console with more details.

4.4. Viewing Java-based Server Details

To display the Details page of a Java-based Server, click the Details button in the Overview page. The server details are displayed in a new dialog, as shown in the following figure:

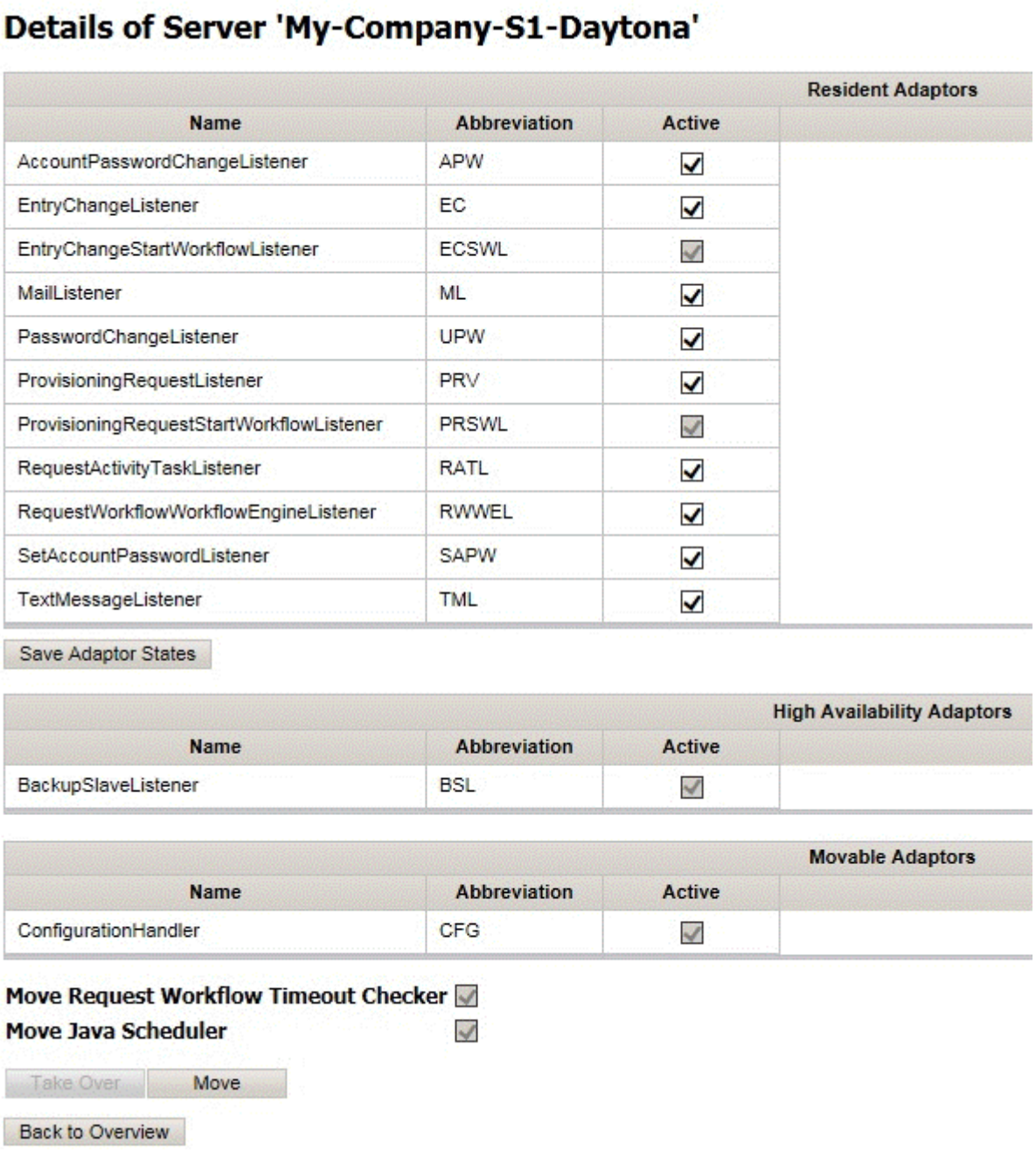

Figure 28. Java-based Server Details Page

The Details page displays the name of the selected Java-based server in the header and some lists of adaptors below it. The Abbreviation column shows the abbreviations for the adaptor names used on the Server Overview page. Adaptors that are not active are assigned to another Java-based Server.

The **Resident Adaptors** are permanently assigned to a server. They can be active or inactive, as indicated by the flag in the **Active** row.

The **High Availability Adaptors** contain only one adaptor, the **BackupSlaveListener**. Its **Active** flag shows whether High Availability is configured for the server.

The **Movable Adaptors** contain only one adaptor, the **ConfigurationHandler**. In contrast to the **Resident Adaptors**, it can exist only on one of the Java based servers.

The **Performs Request Workflow Timeout Checks** check box displayed below the **Movable Adaptors** table indicates whether (checked) or not (unchecked) the selected Java-based Server performs the timeout check for request workflows.

The **Hosts the Java Scheduler** check box displayed below the Movable Adaptors table indicates whether (checked) or not (unchecked) the selected Java-based server hosts the scheduler for Java-based workflows.

On this page, you can take the following actions:

- Click the checkboxes in the Active row of the Permanent Adaptors table and then click the **Save Adaptor States** button to configure the set of active Permanent Adaptors for the Java-based server. Note that some adaptors have a master adaptor. They are automatically activated or deactivated if their master is activated or deactivated.
- Click **Take Over** to move the ConfigurationHandler, the Java scheduler, or the request workflow timeout checker from another Java-based Server to the selected server.
- Click **Move** to move the ConfigurationHandler, the Java scheduler, or the request workflow timeout checker from the selected server to another Java-based Server.

These two buttons are greyed out / disabled if there is nothing to move or take over.

- Click **Back to Overview** to return to the Server Overview page.

4.5. Moving Adaptors

You can move the ConfigurationHandler adaptor to and from servers by clicking the button in the **Move Components** column in the Server Admin Overview page. If a server is running, the direction is "take over", which means that the server will receive the additional adaptors. If a server is down, the direction is "move to", which means that the server will release the adaptor to another server.

The Move Components button is labeled with the related direction (**Take Over** or **Move To**) depending on the server's state. If a move operation is not possible (because the server has already assigned all adaptors or has no adaptor to release), the button is greyed

out/disabled.

You can also initiate an adaptor move from a Java-based Server's Details page by clicking **Take Over** (for the "take over" direction) or **Move** (for the "move to" direction).

When you select to move an adaptor, Server Admin displays the Move Components dialog, as shown in the following figure:

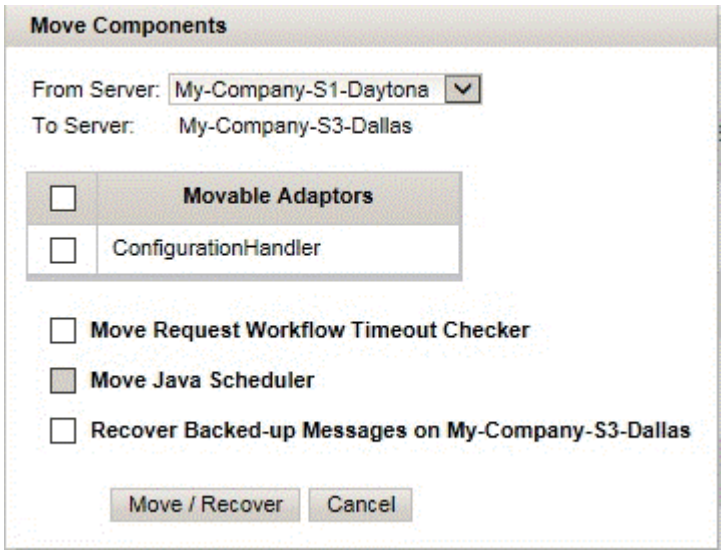

Figure 29. Move Components Dialog

The Move Components dialog displays the names of the **From Server** and the **To Server** for the move. If there is more than one possible server, click the down-arrow to display the list of servers and then click one to select it.

The list of adaptors that are available for move is displayed below the servers. Check the box to the left of an adaptor to select it to be moved. To move the entire list, check the Adaptor heading box.

Check **Move Request Workflow Timeout Checker** to move the timeout checker for request workflows to the target server.

Check **Move Java Scheduler** to move the Java scheduler.

Check **Recover Backed-up Messages on To Server** to start the recovery of backed-up messages on the **To Server**.

Click **Move / Recover** to move the selected components from the **From Server** to the **To Server** or to start a message recovery. Click **Cancel** to exit the dialog without doing anything.

4.6. Moving the Request Workflow Timeout Checker

Moving the timeout checker for request workflows is done from the Move Components dialog, as described in "Moving Adaptors". To move the timeout checker, check **Move**

Request Workflow Timeout Checker in the Move Components dialog. Note that this check box is only activated when the checks are currently performed on the **From Server**.

4.7. Moving the Java Scheduler

Moving the scheduler for the Java-based workflows is done from the Move Components dialog, as described in "Moving Adaptors". To move the Java scheduler, check **Move Java Scheduler** in the Move Components dialog. Note that this check box is only activated when the **From Server** is the current Java scheduler host.

4.8. Moving Tcl Workflows

You can move the Tcl Workflows by clicking the button in the **Move Tcl Workflows** column in the list of C-Servers on the Server Admin Overview page. If a C-server is running, the direction is "take over", which means that the server will receive the Tcl Workflows. If a server is down, the direction is "move to", which means that the C-server will release the Tcl Workflows to another C-server.

The Move button is labeled with the related direction (**Take Over** or **Move To**) depending on the server's state.

When you select to move the Tcl Workflows, Server Admin displays the Move Tcl Workflows dialog, as shown in the following figure:

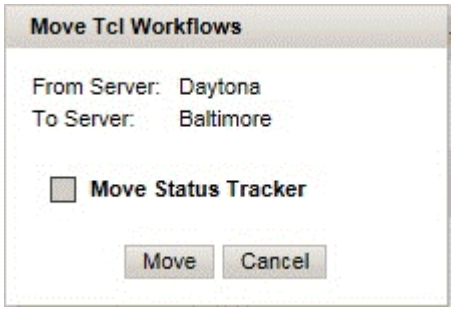

Figure 30. Move Tcl Workflows Dialog

It shows source- and destination C-Server names.

Check **Move Status Tracker** to move the status tracker to the target server. This flag is selectable only if the status tracker resides on the source server.

Click **Move** to move the Tcl Workflows from the **From Server** to the **To Server**. Click **Cancel** to exit the dialog without moving anything.

4.9. Viewing Message Broker Details

To display the Message Broker's Web Console, click the **Start console** button. The Message Broker details are displayed in a new tab, as shown in the following figure:

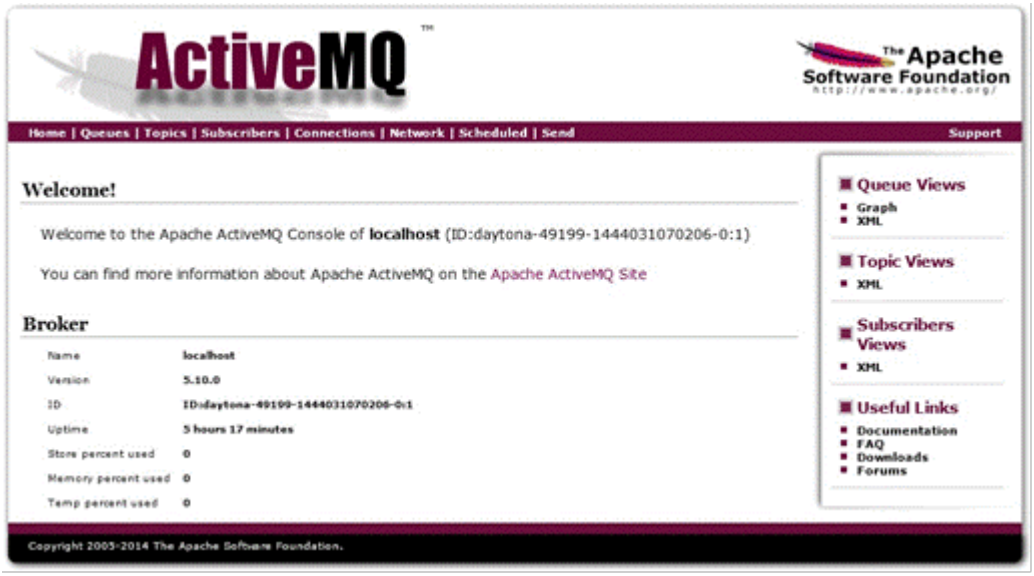

Figure 31. Message Broker JMX Console

This is the standard Apache ActiveMQ Web Console. It provides all information about message broker operation; for example, a topic overview, as shown in the following figure:

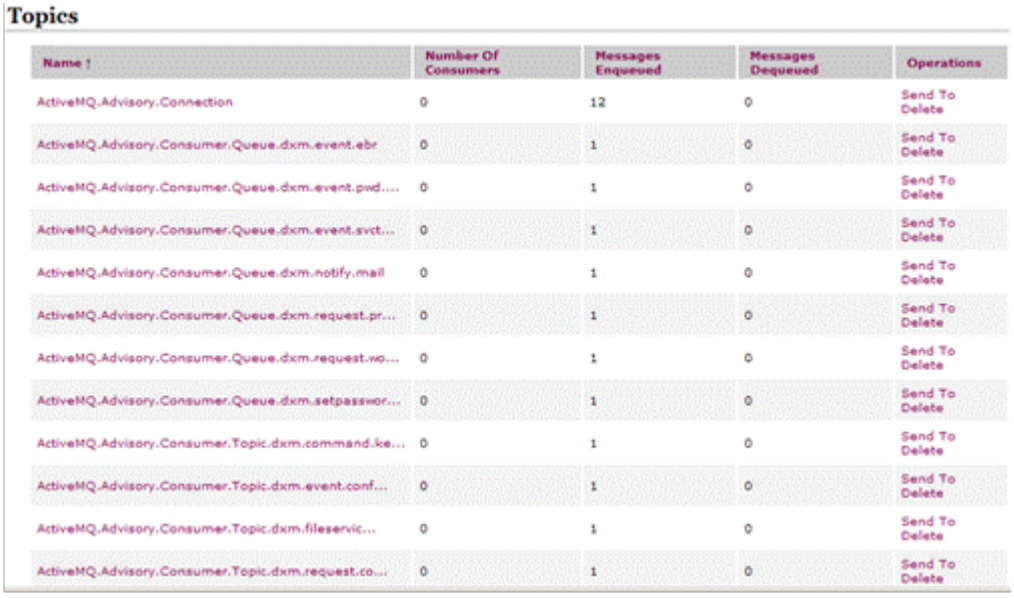

Figure 32. Message Broker Web Console - Topic Overview

The same information is available for queues and other details.

5. Using DirX Identity Web Admin

You can manage the DirX Identity Java-based Server completely through Web interfaces. Because the server interfaces are compatible with the JMX standard, you can use any JMX-compliant application to verify the status of the server or control its operation.

DirX Identity allows you to perform Web-based server administration through:

- DirX Identity Web Admin, which is a specialized administration interface that allows you to verify and control the Java-based Server and also monitor the C++-based Server.
- Any JMX application, which permits you to use your favorite JMX console to control the Java-based Server.

The topics in this chapter provide usage information about Web Admin and explain how to configure a JMX-compliant application to manage a Java-based Server.

5.1. Logging In (Web Admin)

To log in to Web Admin in non-SSL mode, start your browser and then enter the following URL:

http://*server*:_port_**/admin**

For example:

```
http://myserver:40000/admin
```

where **myserver** is the machine where your Java-based (IdS-J) server runs and **40000** is the port that you entered during initial configuration.

If you selected SSL for the Java-based Server during configuration, use the following URL to log in securely to Web Admin:

https://*server*:_port_**/admin**

For example:

```
https://myserver:40443/admin
```

where **myserver** is the machine where your Java-based (IdS-J) server runs and **40443** is the port that you entered during initial configuration.

Web Admin displays a login dialog that requests username and password (default: admin / wE3!dirx).

5.2. About the Web Admin Page Layout

The following figure shows the Web Admin page layout:

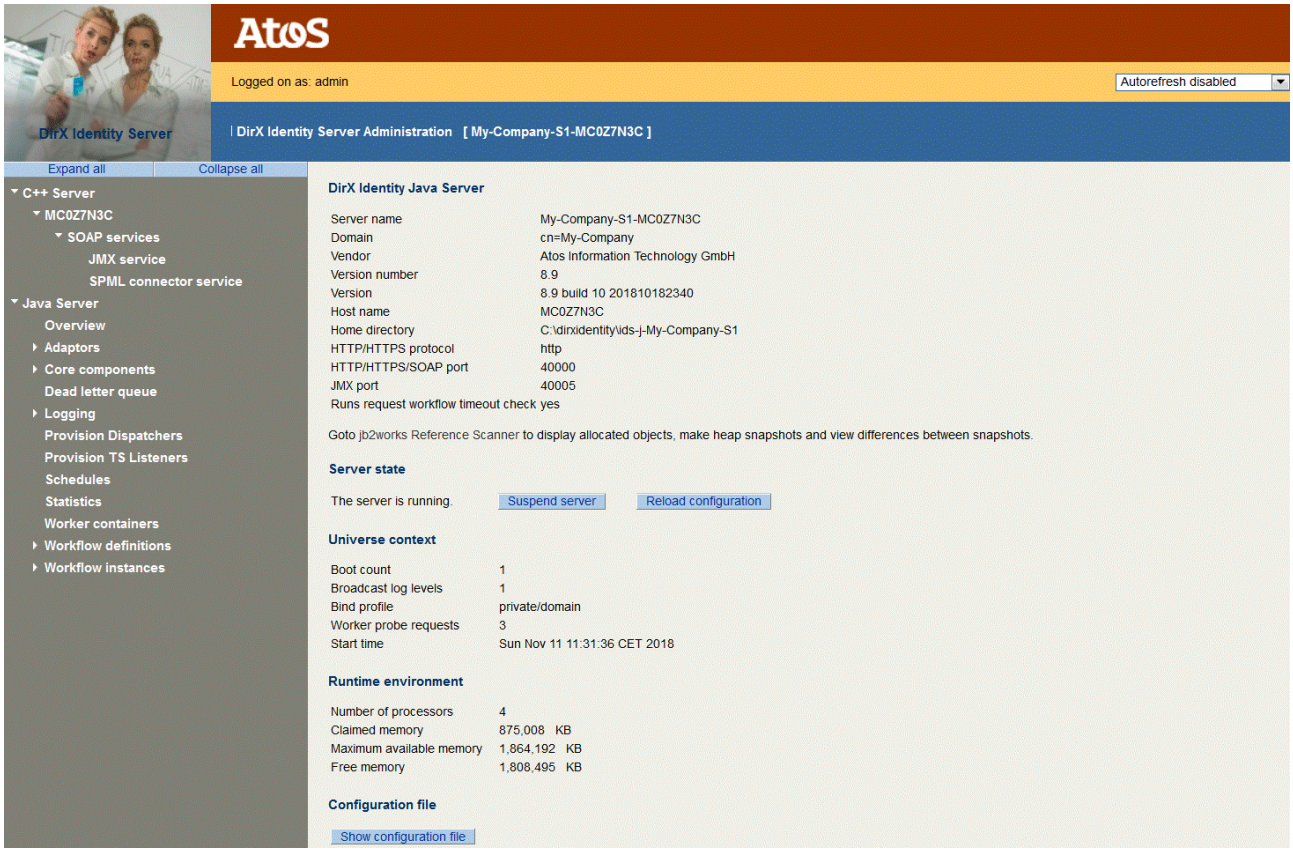

Figure 33. Web Admin Page Layout

As shown in the figure, the default page layout consists of a header at the top, a footer at the bottom (not visible in the figure) and a navigation pane on the left-hand side.The rest of the page is application-specific.

All pages contain the same header, which consists of:

- A company logo and company name
- Information about the user login status, which is either **Not logged on** or **Logged on as**: *username*
- An **autorefresh chooser** field - Click the arrow button and select your desired option. Note: This option is only valid for the current page. It is automatically reset after an action or page change.

The navigation pane consists of a list of nodes that represent a Java-based Server and a C++-based Server.

Note: This version of Web Admin supports only one Java-based server node and one C++-based Server.Use the Server Admin for multiple servers or multiple instances of the Web Admin to control multiple server instances.

Items with a leading triangle contain a sub-structure.Click the triangle to open or close the sub-structure.

Use the **Expand All** and **Collapse All** buttons to open or close all sub-structures.

The footer of the page contains the application version number on the left and other useful

maintenance information.

The next sections explain the sub-structure of the different server types.

5.3. Using the C++-based Server Menu

When you open **C++-based Server** in the navigation pane, Web Admin displays a list of services contained in the primary C++-based Server that you can manage.Click a server node to manage the following services:

- SOAP services - the list of SOAP services for the C++-based Server.

5.3.1. SOAP Services

This selection displays information about the C++-based Server's SOAP services.The **JMX service** handles all requests for maintenance; the Java-based Server uses it to send maintenance requests to the C++-based Server and to receive the response information.The **SPML connector service** handles all messages to and from the connector service.

Each SOAP service selection displays the following information:

- **Port** - the port number the Java-based Server uses to access the C++-based Server to exchange information.
- **Accept timeout** - the amount of time to wait for the accept information of a sent SOAP message.
- **Receive timeout** - the amount of time to wait for the receive message of a sent SOAP message.
- **Current thread count** - the current number of threads running for this service.
- **Busy thread count** - the current number of busy threads.
- **Thread count high water** - the maximum number of threads allowed for this service.

5.4. Managing the Java-based Server

In the Web Admin navigation pane, you can handle:

- Java Server - the top-level node represents the server itself, its state and loaded configuration.
- Overview - shows an overview of the most important parameters.
- Adaptors - components that control various event input channels.
- Core components - global server components.
- Dead letter queue - keeps all events that were not successful for viewing and reprocessing.
- Logging - allows setting log levels and viewing log files.
- Provisioning Dispatchers - special JMS adaptors that read messages for running

Provisioning workflows.

- Provisioning Target System Listeners - read messages for provisioning target systems that should be processed only on dedicated servers.
- Resolution Adapter - resolves users.
- Schedules - shows all running schedules. The full checker runs as the default scheduler.
- Statistics - displays server statistics information.
- Worker containers - the available worker threads.
- Workflow definitions - the list of active workflows loaded into the server and waiting for events.
- Workflow instances - running workflows and schedules.

5.4.1. Managing the Server State

The Server State page allows you to control the Java-based server state and provides the following sections:

- **DirX Identity Java Server** - provides general information.
- **Server State** - displays information about the server state and allows you to manage the server.
- **Universe Context** - shows boot information.
- **Runtime Environment** - displays information about the memory and processors.
- **Configuration File** - displays the current loaded and resolved server configuration in XML format.

5.4.1.1. DirX Identity Java Server

The general information provided is:

The **Server name**.
The **Domain**.
The **Vendor**.
The **Version number**.
The **Version**.
The **Host name**.
The **Home directory**.
The **HTTP/HTTPS protocol**.
The **HTTP/HTTPS/SOAP port**.
The **JMX port**.
The **Run request workflow timeout check** flag.

5.4.1.2. Server State

The Server State area displays the following fields and buttons:

The server is ... - whether the server is running or suspended.
Click **Suspend Server** to suspend the server, click **Resume Server** to start it again.

Click **Reload Configuration** to reload the workflow configuration from the LDAP configuration database (this action has same effect as using the Load IdS-J Configuration selection from the context menu of a server or workflow item in the DirX Identity Manager).

5.4.1.3. Universe Context

The Universe Context area displays the following boot information:

Boot count - the number of server starts on this machine.*
Broadcast Log Levels* - the number of times the log level has changed.*
Bind profile* - the folder that contains the domain bind credentials.*
Worker probe requests* - the number of times the worker threads of the server have been polled.*
Start time* - the time at which the server was last started.

5.4.1.4. Runtime Environment

Displays information about memory and processors:

Number of processors - the number of available processors on this machine.*
Claimed memory* - the amount of memory already claimed by the server process.*
Maximum available memory* - the maximum amount of available memory.*
Free memory* - the amount of memory that is still available.

5.4.1.5. Configuration File

Click **Show configuration file** to display the current server configuration in XML format. All references (visible in the DirX Identity Manager if you view the server configuration) are resolved here.

5.4.2. Overview

The Overview page displays the most important parameters. Follow the link (underlined text strings) to display details. The information displayed is:

- **State** - information about the server state. Click the link to view details.
- SEVERE - the number of severe errors that have occurred since server start. Click the link to view the server log files. (See the section "View log files" for details).
- WARNING - the number of warnings that have occurred since server start. Click the link to view the server log files. (See the section "View log files" for details).
- **Memory** - the maximum memory configured and the amount that is currently consumed.
- **Pending Requests** - the maximum number of pending requests configured and the number currently used.
- **Workflows** - the number of workflow instances. View the Workflow Instances section for details.
- **Retry** - the number of workflow instances waiting for retry. These instances wait due to a recoverable error that has occurred. Click the link for details.

- **DeadLetterQueue** - the number of entries in the dead letter queue. Click the link to display information about the dead letter queue. (See the section "Dead Letter Queue" for details.)
- **Audit channel** - the number of audit requests waiting at the audit channel.
- **Logging channel** - the number of logging requests waiting at the logging channel.
- **Adaptor** - a summary of all configured adaptors. In the **Pending Requests** column, you can see the configured maximum number of requests and the currently available ones. Click the link to view the details of this adaptor. (See the corresponding adaptor section for details.)
- **Resource Family** - the workers that are configured for a specific resource family. The **Tasks** column displays the number of waiting tasks (for example, a batch of password changes). In the **Workers** column, worker icons in green indicate running threads; worker icons in gray are waiting threads. Click the link to display the table of workers. (See the section "Worker Containers" for details.)

The server writes snapshots of this page in HTML format as separate files (**snapshot-***timestamp-counter***.html**) onto disk into the folder *install_path***\logs\overview**. Use the parameter **Maximum No. of Overview Files** in the tab **Status and Auditing** of the Java-based Server object in the **Connectivity** view group of the DirX Identity Manager to control the maximum number of files.

Each time you open or refresh the Overview page, a snapshot file is written. Use the Autorefresh feature to write pages regularly, for example each 5 minutes. This action allows you to view the server history later on. Click the link at the top of the table to view the list of overview files.

5.4.3. Managing Adaptors

Adaptors listen for incoming events and pass them to the JavaSpace for processing. Adaptors exist for external and internal events, including:

- **Account Password Change Listener** - listens for account password changes.
- **Admin Request Handler** - handles all administrative requests.
- **Backup Slave Listener** - listens for all JMS events and stores them in its repository until the events are processed (active only if High Availability is enabled).
- **Configuration Handler** - handles requests from Windows Password Listeners.
- **Entry Change Listener** - listens for entry changes.
- **Entry Change Start Workflow Listener** - listens for events starting event-based processing workflows; can be active only if the Entry Change Listener is also active.
- **Import to Identity Listener** - listens for events that indicate a change in an entry in a remote system (for example, a user in an Active Directory) that needs to be imported into the DirX Identity domain.
- **Mail Listener** - listens for notification events (mail requests).
- **Password Change Listener** - listens for external password change events.

- **Provisioning Request Listener** - listens for provisioning request events for real-time workflows.
- **Provisioning Request Start Workflow Listener** - listens for events starting Provisioning workflows; can be active only if the Provisioning Request Listener is also active.
- **Request Activity Task Listener** - listens for events intended to start an activity in a request workflow.
- **Request Workflow Workflow Engine Listener** - listens for events from external or any other Java-based Server to trigger the workflow engine component.
- **Set Account Password Listener** - listens for account password change events.
- **Text Message Listener** - listens for text message events (SMS requests).

5.4.3.1. Adaptor States

Adaptors can have the following states:

- **Listening** - The adaptor listens for incoming events.
- **Waiting** - The adaptor is blocked because the high water mark has been exceeded. It waits until the low water mark is reached.
- **Suspended** - The adaptor is blocked due to administrator's intervention.

Temporary states are:

- **Recovering** - the adaptor is reading events from the persistent repository after server start.
- **Recovered** - the adaptor has finished reading events. It's going to state **Listening**.
- **Terminating** - the adaptor is stopping.
- **Terminated** - the adaptor is stopped.

5.4.3.2. Account Password Change Listener

Entry Change Listener

Entry Change Start Workflow Listener

Import to Identity Listener

Mail Listener

Password Change Listener

Provisioning Request Listener

Request Activity Task Listener

Provisioning Request Start Workflow Listener

Request Activity Task Listener

Request Workflow Workflow Engine Listener

Set Account Password Listener

Text Message Listener

The Account Password Change Listener listens for account password change events.

The Entry Change Listener listens for entry change events.

The Entry Change Start Workflow Listener listens for messages to start event-based processing workflows.

The Import to Identity Listener listens for events that indicate changes to entries in remote systems that must be imported into the DirX Identity domain.

The Mail Listener listens for notification events.

The Password Change Listener listens for password change events.

The Provisioning Request Listener listens for Provisioning requests.

The Provisioning Request Start Workflow Listener listens for messages to start Provisioning workflows.

The Request Workflow Workflow Engine Listener listens for events to trigger the workflow engine component.

The Set Account Password Listener listens for account password change events.

The Text Message Listener listens for text message events (SMS requests).

Web Admin displays a message that indicates whether the listener is running or suspended. Click **Suspend** or **Resume** to stop and start the adaptor.

The properties of these components are:

- **State** - the state of this listener. (See the section "Adaptor States" for details.)
- **Is Persistent** - whether the listener stores received events in its persistent repository until processing is finished.
- **Number of sent requests** - the number of requests sent to the JavaSpace for processing since the last server start.
- **Number of received responses** - the number of responses for sent requests received from processing workflows since the last server start.
- **Number of outstanding responses** - the number of current outstanding responses for sent requests received from processing workflows. This field indicates the number of events that are not yet finished.
- **Host** - the host name where the server runs.
- **Port** - the port where the server runs.
- **Client ID** - the listener's client ID.
- **Subscription ID** - this server's subscription identifier to specific messages. If the listener receives messages from a queue, the subscription ID is not set.
- **Character set** - the expected character set for the sent requests.
- **Topic** - the topic associated with the listener's function.
- **Retry interval (in milliseconds)** - the connection loss time between two re-connects.
- **High watermark** - the number of outstanding requests after which the listener stops operation. The listener resumes operation when the low watermark is reached.
- **Low watermark** - the number of outstanding requests after which the listener resumes operation after a high watermark is reached.

5.4.3.3. Backup Slave Listener

The backup slave listener listens for all JMS events in a High Availability environment. JMS adaptors of the monitored Java-based Server send a copy of all incoming events (called **add events**) to the backup slave listener. When the event is processed, a delete event is sent to the backup slave listener to delete the event from its repository. If the other Java-based Server fails, the replicated events can be replayed.

Web Admin displays a message that indicates whether the listener is running or suspended. Click **Suspend** or **Resume** to stop and start the adaptor.

The properties of this component are:

- **State** - the state of this listener. (See the section "Adaptor States" for details.)
- **Is Persistent** - whether the listener stores received events in its persistent repository until processing is finished.
- **Number of received ADD events** - the number of events sent to the listener for storing since the last server start.
- **Number of received DEL events** - the number of events for deleting them in the local

repository since the last server start.

- **Number of replayed events** - the number of replayed events since the last server start.
- **Host** - the host name where the server runs.
- **Port** - the port where the server runs.
- **Client ID** - the listener's client ID.
- **Subscription ID** - this listener's subscription identifier.
- **Character set** - the expected character set for the sent requests.
- **Topic** - the topic associated with events to backup.
- **Retry interval** (in milliseconds) - the connection loss time between two re-connects.

5.4.3.4. Admin Request Handler

The admin request handler listens for requests for configuration updates and processes them.

Web Admin displays a message that indicates whether the adaptor is running or suspended. Click **Suspend** or **Resume** to stop and start the adaptor.

The properties of this component are:

- **State** - the state of this listener. (See the section "Adaptor States" for details.)
- **Number of sent requests**- the number of events sent to the JavaSpace for processing since the last server start.
- **Number of received responses**- the number of responses for sent requests received from processing workflows since the last server start.
- **Host** - the host name where the server runs.
- **Port** - the port where the server runs.
- **Client ID** - the listener's client ID.
- **Character set** - the expected character for the request.
- **Topic** - the topic associated with configuration changed event messages.
- **Retry interval (in milliseconds)** - the interval between two accesses to the messaging service. Set it accordingly.

Click **Save** to save changes. Click **Reset** to discard changes and re-set all values to the most recently saved values.

5.4.3.5. Configuration Handler

The configuration handler listens for requests from components that need a current certificate a list of messaging services. The list of messaging services is also broadcast per scheduler.

Web Admin displays a message that indicates whether the adaptor is running or suspended. Click **Suspend** or **Resume** to stop or start the adaptor.

The properties of this component are:

- **State** - the state of this listener. (See the section "Adaptor States" for details.)
- **Number of sent requests** - the number of certificate requests that were read from the messages queue; for example, from the Windows Password Listener.
- **Certificates sent** - the number of certificates published as result of received requests.
- **Host** - the host name where the server runs.
- **Port** - the port where the server runs.
- **Client ID** - the listener's client ID.
- **Subscription ID** - this server's subscription to request certificate messages.
- **Character set** - the expected character set for the sent requests.
- **Topic** - the topic associated with certificate request publications.
- **Broadcast topic** - the topic the certificate handler uses to publish changed certificates.
- **Retry interval (in milliseconds)** - the interval between two accesses to the messaging service. Set it accordingly.
- **Broadcast interval (in minutes)** - the interval between two broadcasts of the list of messaging services. Set it accordingly. This property is only shown for the Configuration Handler.

Click **Save** to save the changes. Click **Reset** to discard the changes and re-set all values to the most recently saved values.

5.4.4. Provisioning Dispatchers

Provisioning dispatchers read messages for provisioning target systems and dispatch them either to the appropriate target system-specific queue or to the respective default queue (for example, *domain**.dxm.request.provisiontots._default*).

For each of the provisioning queues, the detail page shows the number of messages that have been received, how many of them could not be dispatched due to an error, how many have been dispatched and whether to the default or to a target system-specific queue.

5.4.5. Provisioning Target System Listeners

Listeners specific to a target system read and process messages for that target system. If there is no target system, the messages apply to the connected directory. The listeners are started only on the dedicated servers. The number of listeners per queue depends on the configuration of the connected directory.

For each target system, the detail page shows the listeners for three queues (**dxm.request.provisiontots**, **dxm.request.workflow.provisioning**, **dxm.setpasswordrequest**) with the following counters:

- **Messages Received** - the total number of messages received.
- **Messages Re-Delivered** - how many messages were re-delivered due to failure.

- **Messages Failed Temporary** - how many messages failed temporarily. When a failure is considered to be temporary, the listener tries to re-deliver it to process it after the retry time has expired.
- **Messages Failed Final** - how many messages failed finally. A message fails finally if the error is not temporary or the maximum number of retries has been reached.

The queue names are suffixed with a target system identifier. It is built using the attributes type, cluster and domain of the target system in lower case: *type.cluster.domain*. For a target system that is part of a cluster, the domain part is empty and the target identifier is built as *type.cluster*. For more information on this topic, see the chapter “Managing DirX Identity Servers” → “Distributed Deployments and Scalability” → “Separating Traffic for Selected Target Systems” in the *DirX Identity Connectivity Administration Guide*.

5.4.6. Resolution Adapter

The resolution adapter is a JMS adapter that is responsible for resolving users. It listens to JMS messages in the queue *domain**.dxm.request.user.resolve*.

The WebAdmin detail page allows you to monitor the adapter and shows the following fields, mostly counters. Note that the adapter registers a number of listeners at the queue. This is configured in the domain configuration entry.

- **Connected** - whether the adapter is currently connected to the Message Broker.
- **Connection starts** - how often the adapter has started a JMS connection.
- **Exceptions received from JMS connection** - how many exceptions have been received from the Message Broker. Such an exception typically means that the JMS connection is lost.
- **JMS re-bind attempts** - how often the adapter has tried to re-bind to the Message Broker after the connection was lost.
- **Messages Received** - the total number of messages that have been received.
- **Messages Succeeded** - how many messages have been processed successfully and resolved the user.
- **Messages Re-Delivered** - how many messages were re-delivered due to failure.
- **Messages Failed Temporary** - how many of them failed temporarily. When a failure is considered to be temporary, the adapter tries to re-deliver it to process it after the retry time has expired.
- **Messages Failed Final** - how many of them failed finally. A message fails finally if the error is not temporary or the maximum number of retries has been reached.
- **Messages Ignored** - how many of the received messages were ignored. A message is ignored if the user already has been resolved after the change that this message represents. Note that the message contains the time of the change. The adapter adds a grace period to cope with potential time differences at client and server.

5.4.7. Managing Core Components

This section shows detailed information about the internal state of the server.

5.4.7.1. Space

This section shows information about the internal workspace of the server that is only important for debugging purposes. It lists the entries currently stored in the JavaSpace repository of the server. The JavaSpace is a persistent repository that holds all requests and responses exchanged internally between all the server components and the attached workers.

The view represents a snapshot of the active communication channels and workers and of the requests waiting for processing. They are ordered according to their types (their class names).

5.4.8. Dead Letter Queue

If no error activity is configured for a workflow or a failed request cannot be processed by the workflow, the request is placed in the Dead Letter Queue. This part of the Java-based Server administration interface allows you to view the failed requests and responses and to delete them or to process them again.

Web Admin displays a message that indicates whether the adaptor is running or suspended. Click **Suspend** or **Resume** to control the adaptor.

The first section of properties shows the status of the queue:

- **State** - the state of this listener (listening or suspended).
- **Is Persistent** - whether or not received events are stored in its persistent repository until processing is finished.
- **Number of stored requests** - the number of failed requests that are stored here in the internal queue.
- **Number of sent requests** - the number of requests that were re-sent to the workflow dispatcher and removed from the dead letter queue as well.
- **Number of received responses** - the number of requests the workflow dispatcher has processed successfully after re-sending them to the dispatcher.
- **Number of outstanding responses** - the number of (pending) requests the workflow dispatcher is processing.

The next two items let you control the maximum number of requests in this queue:

- **High water mark** - if the number of outstanding requests is higher than this limit, the listener stops working. It starts again when the low water mark is reached. Set it accordingly.
- **Low water mark** - the listener starts working again if the number of outstanding requests is lower than this limit. Set it accordingly.

Click **Save** to save the changes and **Reset** to discard the changes and to re-set all values to the most recently saved values.

You can view, process, or delete stored requests. Define a filter to get a part of the stored requests:

- **Topic** - the filter for topics to work on. You can use the asterisk (*) as a wildcard sign. It is not possible to enter a NOT expression.
  For an explanation of topic formats, see the section "Message Topics" in the *DirX Identity Connectivity Administration Guide*.
- **Time from ... to ...** - the time frame for the requests. Use generalized time formats like **20140108010000Z**.
- **Sort by** - the sort criteria of the search result. Valid values are: **none**, **topic**, **timestamp**, **expires**.
- **Order** - specifies **ascending** or **descending** order.
- **Maximum number of requests** - the maximum number of requests to be retrieved (default: 100).
- **Timeout for processing (sec)** - the time limit for handling search and process commands.

Use **Reset filter** to reset the filter.

Use **Search requests** to generate a list of requests and determine what the errors are. See "Handling the Search Result" below for details.

If you are able to remove the reason for the error - for example, by changing the configuration or re-starting the target system - you can alternatively click **Process requests**. The handler removes the entries from the queue and sends them to the workflow dispatcher, which selects appropriate workflows to process the requests again.

The last part of this page allows you to clear all requests with a specific topic:

- **Topic** - define the topic filter and then click **Clear requests** to remove these requests from the dead letter queue.

5.4.8.1. Handling the Search Result

The result of a search request is displayed in a list. The displayed columns are:

Topic - the topic of the failed event.

Data - three additional columns display more detailed data according to the event type (topic).

Details - the content of this entry in a separate page. For more information see below.

Process - processes this entry again.

Remove - deletes this entry.

The **Details** feature shows these fields of an entry:

Request ID - the internal identifier of this request.

Adaptor Name - the name of the adaptor that delivered this event.

Topic - the complete topic.

Creation time - the time at which this event was received by the adaptor.

UID - a unique internal identifier.

Error code - the error code. Possible values are:

1 (Missing response from workflow: ...) - the workflow dispatcher did not get a response from the workflow or a temporary error could not be resolved via retries.

2 (No workflow found for event, context: ...) - no workflow was found with a matching When applicable section

3 (*specific_message*) - a workflow encountered a specific problem (see the specific_message for more information).

Error annotation - a description of the error code.

Connected directory type - the first variable of the event.

Cluster - the second variable of the event.

Resource - the third variable of the event (named Domain in the DirX Identity Manager).

Identifier - the target of this event (for example, the user DN for a password change or the account or group DN for provisioning events).

Event - the event content itself, in SPML format. Use the **Wrap lines** box to change the display mode of the text box.

Use the **Back to request list** button to return to the request list. Use the  and  buttons to step through the detail pages.

5.4.9. Logging

The Logging section allows you to configure and view server log information, including:

- **Set log levels** - displays all components and lets you set the log levels.
- **View log files** - displays a list of all log files.

See also the "Logging" section in "Managing the Java-based Server" in the *DirX Identity Connectivity Administration Guide*.

5.4.9.1. Set log levels

This subsection displays a list of all relevant components and their current log levels. You can add new components or change the log levels of existing ones.

The fields in the displayed list are:

- **Component** - the component name. Standard components are:
  Default - the default log level if nothing else is specified.
  Activity engine - the engine to control activities.
  Adaptors - the list of configured adaptors.
  Configuration - the configuration manager.
  Connectors - the list of configured connectors.
  Filters - the list of configured filters (for example, the crypto filter).
  Job - the list of configured jobs.
  Scheduler - the scheduler component.
  Space - the workspace handler (JavaSpace implementation).
  Workflow engine - the engine to run workflows.
  Workflow resolver - the component that retrieves the correct workflow for an event.
  Other packages and classes - standard components for logging, auditing, ...
  New package or class - specifies a new package or class
- **Sub component** - the sub component name.
- **Package or class name** - the corresponding Java class package or class.
- **Level** - the log level. Valid values are:
  DEFAULT - default logging level (see note below).
  OFF - no logging.
  SEVERE - severe errors.
  WARNING - severe errors and warnings.
  INFO - severe errors, warnings, and info messages.
  FINE - severe errors, warnings, info messages and fine logging.
  FINER - severe errors, warnings, info messages and finer logging.
  FINEST - severe errors, warnings, info messages and finest logging.
  ALL - all logging activated.

The log levels are arranged in sequential order, each level producing more log entries than the lower one. Level OFF produces no log records at all; SEVERE is for error messages, while FINEST contains debug messages usually comprising the message and configuration data.

The DEFAULT log level is special. The logging can be set for Java classes or package names. A package name is divided into parts separated by a period. All names are structured in a tree. The default log level is specified for the root of the tree. Underneath the root are the package part names like "com", "org", or "siemens". The second node in the tree hierarchy is then, for example, "com.siemens" or "org.apache" and so on. You can set a log level for each node. If not, a log level is set for a class, and then the first node for which a log level is set beginning from the class name to the root defines the effective log level for the class. If no log level is set for any nodes, ultimately the log level is taken from the root (the default log level).

The log settings are stored in a file permanently and survive server restarts.

Use the **New package or class** field to add a new component to the list (for example, a custom connector).

Use **Save** to save the changes and use **Reset** discard the changes and to re-set all values to the last recently saved values. Saving changes takes effect immediately.

Use:

- **Dump all threads** to write all threads with stack trace and deadlock information to the file **webAdminThreadDump.**counter***.txt* in the folder **logs**. It also produces a file **webAdminTasks.**counter***.txt* in the folder **logs** with all tasks currently in the JavaSpace.
- **Dump top threads** to write the 15 top threads that are consuming the most CPU resources to the file **webAdminThreadTop.**counter***.txt* in the folder **logs**.
- **Dump heap** to write a memory heap dump for support diagnosis to the file **webAdminHeap.**counter***.hprof* in the folder **logs**.
- **Dump all loggers** to write a list of all logger objects with detailed information for support diagnosis to the file **webAdminAllLoggers.**counter***.txt* in the folder **logs**.

5.4.9.2. View log files

Displays the complete list of log files from the server log folder.

See also the "Auditing", "Logging" and "Statistics" sections in "Managing the Java-based Server" in the *DirX Identity Connectivity Administration Guide*.

Available fields are:

- **Filename** - the name of the file.
- **Size** - the size of the file.
- **Last modified** - the last modified date.

The displayed files are:

- **diaginfo-**timestamp-counter***.txt* - files that contain diagnosis information for support.
- **classloader.txt** - a file that contains all classes loaded.
- **overview** - a folder that contains snapshots of the Overview page. The file names of the snapshots are **snapshot-**timestamp-counter***.html*. (See section "Overview" for details.)
- **readme.txt** - a read-me file containing the string "Log files go here ..."
- **server-**timestamp-counter***.txt* - server log files.
- **server.xml** - the current configuration with which the server is running.
- **serverstate.txt** - the current server state with information about universe context, global context, loaded workflows, worker containers, and MBeans. By default, this file is re-written every hour. You may change the frequency for your IdS-J server in the **Status and Auditing** tab with DirX Identity Manager.
- **start.log** - the startup logging information, which contains logs written before the

server configuration (containing the log file name) was evaluated.

- **stderr.**{**1**|**2**|**3**}*.log* - redirected output to standard error.
- **stdout.**{**1**|**2**|**3**}*.log* - redirected output to standard out.
- **warning-**timestamp-counter***.txt* - all error and warning log entries from the server log file.

5.4.10. Schedules

This menu entry displays all active schedules. These are timers that control the timeout of workflows and activities and the waiting time for activities that need retry.

The available columns are:

UID - an internal unique ID.

Time - the initial date for this schedule.

Task - information about the task to be performed.

By default, the Full check schedule is displayed. The workflow engine performs the full check to look for non-processed items. These items could exist if events were not correctly processed.

5.4.11. Statistics

The Statistics view shows statistics information since the last server start. It presents a set of counters that typically represent the number of received events and responses and of errors. The counters are reset to 0 when the server starts. See also "Statistics" in "Managing the Java-based Server" in the *DirX Identity Connectivity Administration Guide*.

Statistics are provided for:

- Workflows
- Events
- Realtime workflows
- Request workflows

Workflow Overview

This statistic provides the following information:

- Number of processed workflows.
- Number of resolved tasks.
- Number of severe errors. (See log files for details and search for **SEVERE**.)
- Number of warnings. (See log files for details and search for **WARNING**.)

Event Overview

This statistic provides the following information:

- Number of requests.
- Number of outstanding responses.
- Number of supplemented responses.
- Minimum duration.
- Maximum duration.

Realtime Workflows

This statistic provides the following information:

- **Name** - the name of the workflow.
- **Start** - the number of workflows that SUCCEEDED and the number of workflows that FAILED.
- **Event** - the number of events that SUCCEEDED and the number of events that FAILED.
- **Search** - the number of search operations that SUCCEEDED and the number of search operations that FAILED.
- **Add** - the number of add operations that SUCCEEDED and the number of add operations that FAILED.
- **Modify** - the number of modify operations that SUCCEEDED and the number of modify operations that FAILED.
- **Delete** - the number of delete operations that SUCCEEDED and the number of delete operations that FAILED.
- **UpToDate** - the number of objects that were already up to date (no operation necessary).

Request Workflows

This statistic provides the following information:

- **Name** - the name of the request workflow.
- Workflows
- **Started** - the number of request workflows that were started.
- **OK** - the number of request workflows that succeeded.
- **Failed** - the number of request workflows that failed.
- **Other** - the number of request workflows with another status.
- Activities
- **Started** - the number of activities that were started.
- **Running** - the number of activities that are in state RUNNING.
- **OK** - the number of activities that succeeded.
- **Failed** - the number of activities that failed.

5.4.11.1. Details

This section explains the details that are displayed if you click on a line in either the **Real-time Workflows** or **Request Workflows** table above.

Details for Realtime Workflows

- Workflow Starts and States
- **Started** - the total number of workflows started (sum of Succeeded and Failed fields).
- **Succeeded** - the total number of workflows that succeeded.
- **Failed** - the total number of workflows that failed.
- **UpToDate** - the total number of up to date operations.
- Event and Operations
- **Name** - the operation name.
- **Events Processed** - the number of succeeded and failed events.
- **Operations Performed** - the number of succeeded and failed operations.

Details for Request Workflows

- Workflow Starts and States

Lists counters for each status that occurred.

- Activities

Lists counters for each activity / state combination that occurred.

5.4.12. Worker Containers

This section displays all running worker threads in this server. The columns in this list are:

- **Host** - the host where either the server or the worker container runs.
- **Worker Container** - a block of information for each worker container.

The first line of each Worker Container block provides the following information:

- *Worker container name* - the name of the worker container (**colocated** represents the worker container running in the server itself).
- *Identifier* - an internal unique identifier for this worker container.

The Worker Container block shows:

- *Worker name* - the worker container name and a thread number.
- *Resource family* - the resource family for which this thread is waiting. Possible values are:
  {workflowengine} - the resource family is reserved for the workflow engine itself, which starts and controls workflow activities.

{scheduler} - the internal scheduler of the server, which handles timeout situations and triggers retry of activities.
{**workflowscheduler**} - the scheduler for real-time workflow schedules.
{*resource family*} - the specific resource family for which this thread is configured. You can configure the resource families and the number of threads for a Java-based Server at the corresponding configuration object in the Connectivity view (note that changing these parameters requires a restart of the corresponding Java-based Server).

- *Status* - one of the following values:
  waiting for task - the thread is ready to take the next task._
  identification of running task_ - this thread is currently running.

Watching this list, you can see the running and waiting worker threads. You can configure the resource families and the number of threads for a Java-based Server at the corresponding configuration object in the Connectivity view (note that changing these parameters requires a restart of the corresponding Java-based Server).

The details button  allows you to reduce the number of worker threads or create additional ones temporarily. This information is lost after Java-based Server restart.

After clicking the details button, these fields are displayed:

- **Host** - the host where this worker container is running.
- **VMID** - the internal unique ID of the Java virtual machine of this worker container.
- **Resource Family** - the resource family with which the new thread works. Note that resource family names are case-sensitive.

Click **Add** or **Remove** to add or remove threads of this resource family type.

The **Action** field displays the number of threads that will be added or removed.

Click **Save** to perform the displayed action (creating the new worker threads and deleting worker threads). Click **Cancel** to go back to the **Workers** list without performing any action.

5.4.13. Workflow Definitions

This menu entry shows all loaded (active) workflow definitions. Three types of definitions can be available:

Realtime workflows - shows real-time workflow definitions.

Request workflows - shows request workflow definitions

Open the tree structure (click the triangles) to view the loaded definitions. The tree structure is identical to the folder structure visible in the DirX Identity Manager. Clicking a leaf node (there is no triangle before the entry) displays these fields:

5.4.13.1. Workflow Details

This subsection displays the configuration of all configured workflows. These fields are displayed:

- **Workflow Name** - The (LDAP) path of the workflow in the Connectivity configuration.
- **Configuration Manager** - The configuration manager class that loaded the definition.
- **Definition** - The complete loaded (active) workflow configuration definition in XML format. This field allows you to check whether all parameters are set correctly after references are resolved.

5.4.14. Workflow Instances

This menu entry shows all workflow instances for the following types of workflows:

Real-time Workflows - shows the real-time workflow instances.

Request Workflows - shows the request workflow instances.

When you select a menu item, a dialog is displayed to specify a filter for selecting specific workflow instances. The following sections provide information about:

- Using the filter.
- Information displayed in the workflow instances table.
- Workflow details.

5.4.14.1. Using the Filter

Specify specific parts of the workflow name and path, workflow states and / or a start and / or end time interval for selecting specific workflow instances:

- **Name / Path** - specify a part of the workflow name and / or path.
- **Workflow state** - check or uncheck the states of interest to you. For request workflow instances, use:
- **Select failed** - to select all failed states.
- **Select all** - to select all states.
- **Deselect all** - to de-select all states.
- **Start date / End date** - specify time intervals for start or finish time in the **Started** and **Finished** fields. The end date can be specified only for request workflows. Use:
- **Today** - to specify the current date.
- **Since ... days ago** - to specify a time period in days.
- **Clear** - to delete an interval or date.
- **Limits** - specify the size limit for the search (for request workflows only).

Use:

- **Hide filter** - to hide the filter specification area.
- **Change filter** - to display the filter specification area and change the filter values.
- **Search** - to start the search operation and display the selected workflow instances.

- **Reset -** to discard the changes and to keep the previously specified filter values.

The filter definition remains valid until you restart the browser. After a browser start, all available states are selected and no start or finished in time interval is specified.

5.4.14.2. Workflow Instances Table

When you click **Search**, Web Admin searches the selected workflow instances and displays the result in table format. It displays the following information:

- **Name** - the workflow instance name.
- **Path** - the base components of the path to the workflow definition. The full path is displayed as a tool tip.
- **State** - the state of the workflow instance.
- **Start Time** - the time when the workflow was started.
- **End Time** - the time when the workflow finished (request workflows only).
- **Expiration Time** - the time when the workflow will expire (real-time workflows only).
- **Actions** - possible actions on the workflow instance:
- **Cancel** (**x**) - cancels the workflow instance. The workflow instance goes to state FAILED.ABORTED.
- **Suspend** (**||**) - suspends a running workflow instance. (This does not work for real-time workflows.)
- **Resume** (**>**) - resumes a suspended workflow instance. (This does not work for real-time workflows.)

Use the **Change filter** button to display the filter specification area and search for other workflow instances. (See the section "Using the Filter" for details.)

You can sort the result table by clicking on a column heading.

Click on a list item to display workflow instance details. (See the section "Workflow Details".)

Note that real-time workflow items are only visible while they are running.

5.4.14.3. Workflow Details

The workflow details are displayed below the result table. The following information is provided:

- **Name** - the workflow display name.
- **Path** - the path to the workflow definition.
- **State** - the state of the workflow.
- **Start Time** - the start time of the workflow.
- **End Time** - the time when the workflow finished.
- **Expiration Time** - the expiration time of this workflow instance.

Activities

A table that contains all activities of this workflow. The columns are:

- **Name** - the name of the activity.
- **State** - the state of the activity.
- **Start Time** - the start time of the activity.
- **End Time** - the time when this activity finished.
- **Resourcefamily** - the resource family of this activity.Note that for request workflows, **workflowengine** is always displayed.
- **Retries** - the number of retries already performed and the last retry time.
- **Schedule** - the schedule that started this workflow, if any.
- **Assigned Worker** - the assigned worker, if any.

Use **Hide details** to hide the workflow details.

5.5. Monitoring a Java-based Server with a JMX Application

Java Management Extensions (JMX) is a Java technology that supplies tools for managing and monitoring applications, system objects and service-oriented networks.These resources are represented by objects called MBeans (for Managed Bean).You can use any JMX-enabled client to control the Java-based Server or the Apache ActiveMQ Message Broker.

Note: The C++-based Server is not yet JMX-enabled.

One possible selection is Jconsole from a Java JDK.In this case:

Start the console.

In the dialog box for a New Connection, enter under Remote Process *host*:_port_ (on a local machine, you can enter **localhost** and **40005**), the username **domainadmin** in **username** and the password for the DomainAdmin of the Connectivity store in **password**.Click **connect**.Another dialog box is displayed if you are not using SSL.Click **Insecure connection**.

By default, JMX access for the Java-based Server (IdS-J) is enabled but needs authentication.

5.6. Exposed MBeans for JMX Applications

This section describes the MBeans that are available for the Java-based Server.

In general, an MBean object offers:

- Attributes that can be read (or written)

- Methods that can be invoked and arguments that can be supplied to them or values returned from them

Every MBean has an object name in the format:

domain: *key-property-list*

For the Java-based Server, the *domain* part is **com.siemens.idm**.

5.6.1. Server

Object Name: com.siemens.idm:type=idsj,topic=core,name=Server

Attribute: **State** - an integer value that represents the server state ranging from 0 to 10, where 10 is good. Internally, the state represents the current server's use of heap memory. A value below 4 indicates a server with a high memory load.

Object Name: com.siemens.idm:type=idsj,topic=core,name=Statistics

Attribute: **SEVERE** - the number of SEVERE messages that occurred.

Attribute: **WARNING** - the number of WARNING messages that occurred.

A high number indicates connected directories that have been unavailable for a long period or misconfigured workflows, or other severe issues.

5.6.2. Target System-specific Listeners

Object Name: com.siemens.idm:type=idsj,topic=
ProvTSListener,name=*queueType.type.cluster.resource*

where *queueType* is **provisiontots**, **setpasswordrequest** or **workflow.provisiontots**

and *type.cluster.resource* is taken from the corresponding attributes of the target system.

Attributes:

name - the queue name the adapter is listening to.

messagesReceived - the number of messages received.

messagesSucceeded - the number of messages that were processed successfully.

messagesRedelivered - the number of received messages that were re-delivered; that is, they were processed before but failed temporarily.

messagesFailedTemporary - the number of messages that could not be processed successfully and were re-delivered with a delay.

messagesFailedFinal - the number of messages that could not be processed successfully and where a retry was not possible; for example, because the maximum number of retries was reached.

5.6.3. Adaptors

Object Name: com.siemens.idm:type=idsj,topic=adaptor,name=*AdaptorName*

where *AdaptorName* is, for example, **ProvisioningRequestListener**, **EntryChangeListener**, **DeadLetterQueue**, and so on.

Attribute:*state* - the adaptor's state: listening, waiting, or suspended.

Attribute: **outstandingResponses** - the number of current outstanding responses for sent requests received from processing workflows. This field indicates the number of events that are not yet finished. A high number indicates a heavy load. If the value reaches the high watermark, the adaptor enters the waiting state. Note that this is not a real warning case as the server will process these requests and will reconnect to the message broker when the low watermark is reached and will retrieve further requests. Only if the number is constantly high for a very long period should the situation be considered a warning.

Attribute: **entryCount** - a special attribute for the DeadLetterQueue (DLQ): the number of stored events that could not be successfully processed. A high number indicates connected directories that have been unavailable for a long period, misconfigured workflows or other severe issues.

Attribute: **highWater** - the high watermark value.

Attribute: **lowWater** - the low watermark value.

5.6.4. Dispatchers

Object Name: com.siemens.idm:type=idsj,topic= ProvMsgDispatcher,name= *queueType*

where *queueType* is **provisiontots**, **setpasswordrequest**, or **workflow.provisiontots**.

Attributes:

name - the queue name the dispatcher is listening to.

messagesReceived - the number of messages received.

messagesFailed - the number of messages that could not be forwarded to either the default queue or the target system-specific queue.

5.6.5. Resolution Adapter

Object Name: com.siemens.idm:type=server.extension.adapter,name=resolutionAdapter

Attributes:

JmsConnectionStarted - whether the adapter is currently connected to the Message Broker.

JmsConnectionStarts - how often the adapter has started a JMS connection.

JmsExceptions - how many exceptions have been received from the Message Broker. Such an exception typically means that the JMS connection was lost.

JmsRebinds - how often the adapter has tried to re-bind to the Message Broker after the connection was lost.

MessagesReceived - the total number of messages that have been received.

MessagesSucceeded - how many messages have been processed successfully and resolved the user.

MessagesRedelivered - how many messages have been re-delivered due to failure.

MessagesFailedTemporary - how many messages have failed temporarily. When a failure is considered to be temporary, the adapter tries to re-deliver it to process it after the retry time has expired.

MessagesFailedFinal - how many messages have failed finally. A message fails finally if the error is not temporary or the maximum number of retries has been reached.

MessagesIgnored - how many of the received messages have been ignored. A message is ignored if the user has already been resolved after the change that this message represents. Note that the message contains the time of change. The adapter adds a grace period to cope with potential time differences at client and server.

5.6.6. Realtime Workflows

For each realtime workflow that has run at least once, an object is created with the full workflow name; for example, **Ident_Extranet_Realtime** from the My-Company scenario:

Object Name: com.siemens.idm:type=idsj,topic=core,name=Statistics, name0=My-Company,name1=Main,name2=Target Realtime,name3=Extranet Portal, name4=Ident_Extranet_Realtime

Attribute: **START** - the number of workflow runs.

Attribute: **SUCCEEDED** - the number of succeeded workflow runs. The difference of these 2 values contains failed or running workflows.

Attribute: **WARNING** - the number of workflows with warnings.

Attributes: **join**.**ModifyFailed**, **join**.**AddFailed**, **join.DeleteFailed**, **join.SearchFailed** – each value represents the number of failed request operations. These numbers should be zero or small.

5.6.7. Request Workflows

For each request workflow that has run at least once, an object is created with the full workflow name; for example, **Manager Nomination** from the My-Company scenario:

Object Name: com.siemens.idm:type=idsj,topic=core,name=Statistics,name0=confdb, name1=workflow,name2=Definitions,name3=My-Company,name4=Approval,

name5=Manager Nomination

Attribute: **START** - the number of workflow runs.

Attribute: **SUCCEEDED** - the number of succeeded workflow runs. The difference of these two values contains failed or running workflows.

Attribute: **FAILED** - the number of failed workflow runs.

Attribute: **Apply Changes.SUCCEEDED** - the number of succeeded Apply Changes activity runs.

General Note:

Not every attribute described here is always present. For example, if none of the processed request workflow runs has failed, then the attribute FAILED is not present.

6. Using DirX Identity Utilities

DirX Identity provides a set of utilities necessary for data management. These utilities include:

Transport - a set of tools that allow for the exchange of data between directory servers and domains.

Link Checker - a set of tools that check for broken links and can remove them on request.

Log Merger (**logMerge**) - a tool to merge the workflow-specific log files of several Java-based Servers.

Log Analyzer (logAnt) - a tool to analyze complex Java-based Server log files.

Log Viewer (logViewer) - a tool to analyze complex Web Center log files.

Run Workflow Tool - a tool to start workflows from any location inside the network from the shell level.

Run Report Tool - a tool to start reports from any location inside the network from the shell level

6.1. Transporting Data

Identity management systems require transfer of data under various circumstances.The topics in this section describe DirX Identity's transport mechanism, including:

- Typical application of the transport mechanism
- How to use collections
- Methods for exporting, deleting and importing data
- Transporting data as a Java-based workflow
- Transporting data in batch mode
- How to simulate transport, including comparison of source and target
- Some hints and restrictions you should take into account

You use DirX Identity object collections to define the set of objects you want to transfer from one location to another. The transport mechanism allows you to export collections automatically with schedules and import a set of exported files with additional filtering and mapping of attributes and automated domain mapping.

The sections that follow explain typical applications of the transport mechanism in more detail.

6.1.1. Typical Applications

This section describes typical applications of the transport mechanism:

- Concurrent development in a complex identity project.
- Management of configuration data in a configuration management system (CMS).
- Transport of data between development system, integration / test system and productive system.

6.1.1.1. Using Concurrent Development

Customer scenarios often comprise a large set of functionality. To meet project deadlines, several developers must work in parallel, each one developing a well-defined part of the customer scenario. The concurrent work results are typically consolidated and tested in a **Development system**.

Let's assume that each developer creates workflows to a specific connected system. A proven work procedure for these tasks is:

- In the Connectivity Expert view, define a collection folder under Collections for your project.
- Define a **central collection** that contains all objects that are used by all workflows (for example, the central Identity Store), project folder objects for workflows, jobs and connected directories and multiple-use agent or connected directory type definitions, INI files or scripts. We recommend creating a hierarchy of collections, where each one keeps a specific part of the central data.
- Do not include the channel objects of the Identity Store into the central collection, since these items belong to the individual workflows. Select the Identity Store with all its sub objects, but not with the channel objects, using a rule-based export definition. Ideally, one developer (the central collection developer) should be responsible for these central collections.
- Define a separate collection for each workflow (or set of workflows that connect a specific connected directory). Use folder objects to collect the necessary workflows, jobs and connected directories as sub structures if you want to handle multiple workflows per collection. Each workflow developer has his own collection.

Include the collection object itself into the collections (include it into the **Objects** tab). This step preserves the object and allows it to be used at the target side.

At the beginning of the project, the central collection developer builds the central collection once and distributes it to the workflow developers, who can now work in their private installations of DirX Identity. When a local result is available, the developers deliver their collection to the central **Development system** where it can be consolidated and tested. If necessary, the central collection can be updated at any time to the local sites.

6.1.1.2. Using Configuration Management Systems (CMS)

If you use a **software configuration management** system, you can keep the resulting collection files as separate objects in the configuration management store. Each checkin creates a new version, which makes it easy to reset your work to a consistent state. The following figure illustrates this process.

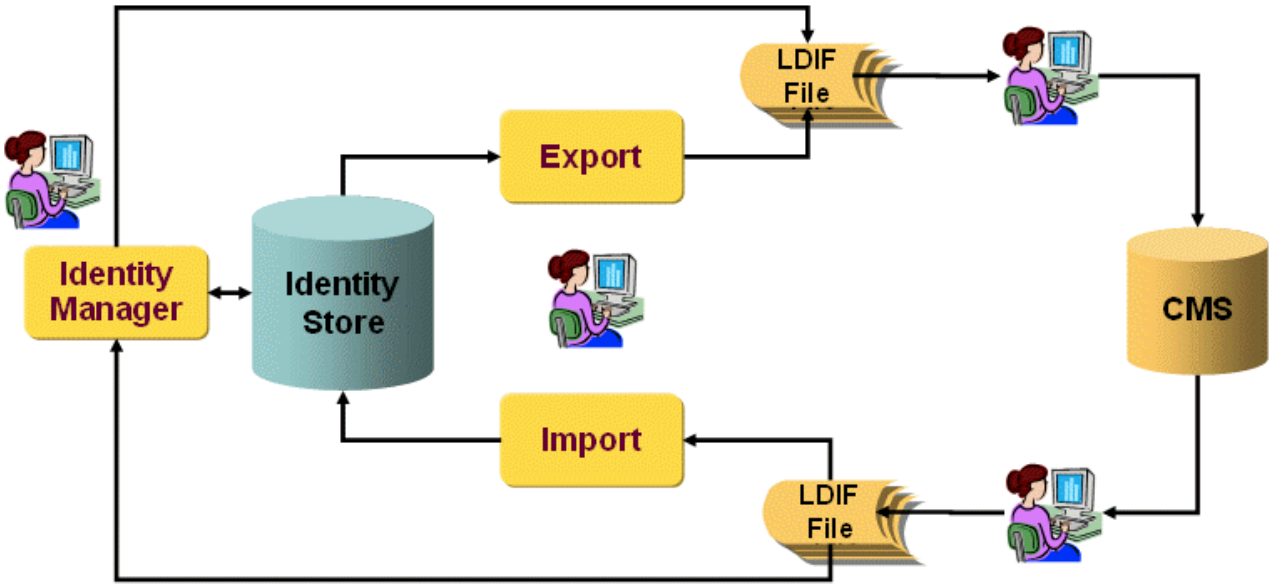

Figure 34. Export and Import to a Configuration Management System (CMS)

If you need a single LDIF file with the complete project content, we recommend that you produce it during production using simple concatenation.

Alternatively, you can define a project collection that contains all of the required collections and exports it into a single file that is checked into the CMS. The disadvantages with this method are that the file may become quite large and that you lose the ability to reset parts of the file individually. So we strongly recommend using separate files.

When working with configuration management systems, you should not generate LDIF files that contain base64 format. For this reason, we recommend that you keep the flag collection.base64 set to FALSE (see the dxi.cfg file or the corresponding setting of a transport export workflow). This setting guarantees that all parts of the collection are visible in clear text format (which is not standard LDIF format and cannot be read by standard LDIF readers). These files can be handled best by configuration management systems that calculate differences from the files to reduce the amount of total disk space and to allow you to view the differences between versions of the same object.

Some configuration management systems cannot handle very long lines (for example, ClearCase). Use the parameter collection.maxlinelength in the file dxi.cfg or the corresponding setting in the transport export workflow. Set collection.maxlinelength to 2000 if you use, for example, ClearCase.

6.1.1.3. Managing Staged Environments

In identity management projects, it is important to separate development, integration and productive systems clearly. In small projects, an integration system might be dispensable. The following figure illustrates this process.

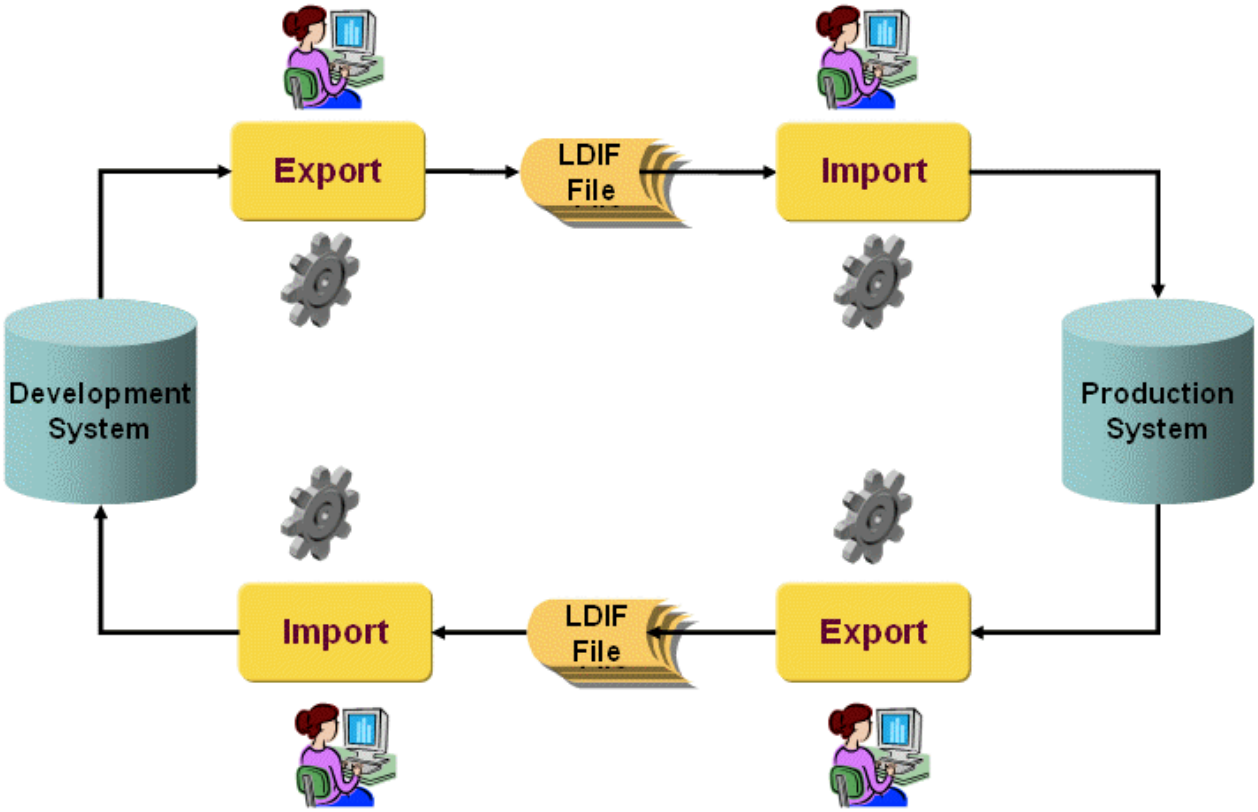

Figure 35. Exchange within a Staged Environment

The figure shows that you can set up an export from one system and an associated import into another system and vice versa. Easy-to-use import features allow you to filter the data accordingly.

In all cases, you transfer the data between these systems as follows:

- Define collections in the source system (for example, the development system) to identify the objects to transfer and the files where the data shall be stored.
- Specify a transport export workflow to export these collections from the source system.
- Define a transport import workflow to import the exported data into the target system (for example, the integration system). The import procedure lets you define domain mapping and attribute mapping operations.

6.1.2. Using Collections

Object collections are an easy way to define a set of objects you want to export from a Provisioning domain or a Connectivity database. You can define single object lists, lists of sub-trees and lists of rule-based object exports. You can also create object collection hierarchies.

6.1.2.1. About Collections

A collection can comprise these object sets:

Objects - a list of single objects.

Subtrees - a list of objects that each comprise a complete sub-tree of objects.

Rule-based - a list of objects that are collected based on a rule-based approach.

Collections - a list of sub-collections, this collection shall include.

To create a new collection:

- Create a new object collection. Right-click the **Collection** folder or one of its sub-folders, and then select **New → Collection**.
- Enter a **Name** and a **Description** for the new object collection.
- Define the path and name of the LDIF file to which the collection is to be written.
- You can define a **set of single objects,** a **set of object trees**, a **set of objects that are exported based on rules** and a **set of nested collections**.
- Save the collection object.

For more information about collections and especially the collection rules, see the context-specific help information in the *DirX Identity Connectivity Administration Guide* and the *DirX Identity Provisioning Administration Guide*.

6.1.2.2. Collection Output Sequence

The output of a collection is sorted to enable comparisons on whole file contents (important for manual or automatic checks). This mechanism guarantees stable output for configuration management systems such as ClearCase.

- First the objects of the collection (as listed at the user interface level) are sorted.
- Next, the sub objects (if a subtree is exported) of one of these objects are sorted.
- Next, the rule based objects are sorted.
- Next, the sub collections are integrated and sorted.
- Next, the attributes within each object are sorted.
- Lastly, the values within a multi-value attribute are sorted.

6.1.2.3. Collection Examples

This chapter provides some examples of object collections. Because collections of single objects and sets of subtrees are easy to define, this section concentrates on rule-based collections.

6.1.2.3.1. Example 1: Tcl-based Workflows (Connectivity View Group)

Tcl-based workflow definitions consist of a complex set of objects and subtrees connected via links. You can export Tcl-based workflows best with DirX Identity's predefined collection rule **Tcl-based Workflows**. You can find this collection rule in **Connectivity** → **Collections** → **Collections Rules** → **Default**. Check the **Content** tab for the definition, which is as follows:

- This definition allows an export of containers (**dxmContainer**) with all their sub nodes.

- Next, it defines that the **dxmActivity-DN** link is used from workflow objects (**dxmWorkflow**) to find all related activities.
- The **dxmRunObject-DN** is used from the activities (**dxmActivity**) to retrieve either workflow objects or job objects.
- The collection takes the job objects (**dxmJob**) and down to a level of three all sub objects (you could also specify 'all' at this point to take the whole subtree). Additionally, the **dxmInputChannel-DN** and the **dxmOutputChannel-DN** links are used to find all related channels.
- All **dxmSelectedFile-DN** are used from the channels (**dxmChannel**) to retrieve potential file definitions.
- The last definition excludes all Java-based channels (**dxmChannelDefinition**).

These objects define the entire workflow with all of the required channels but without the two connected directories at both endpoints. Use this template and adapt it to your needs.

6.1.2.3.2. Example 2: Java-based Workflows (Connectivity View Group)

Java-based workflow definitions consist also of a set of objects and subtrees that are only partially connected via links. You can export Java-based workflows best with DirX Identity's predefined collection rule **Java-based Workflows**. You can find this collection rule in **Connectivity** → **Collections** → **Collections Rules** → **Default**. Check the **Content** tab for the definition, which is as follows:

- This definition allows an export of containers (**dxmContainer**) with all their sub nodes.
- Next, it defines to take all workflow objects (**dxmIDMWorkflowDefinition**) together with the next level, the activities.
- Together with the activities (**dxmIDMActivityDefinition**), it retrieves the port objects and follows the **dxmBindProfile-DN**.
- The collection takes the port objects (**dxmPortDefinition**) and follows the **dxmSpecificAttributes:channelparent** link to retrieve the channels.
- The definition takes all channels (**dxmChannelDefinition**), including the next level of objects (the mapping objects).
- The last definition excludes all Tcl-based channels (**dxmChannel**).

These objects define the entire workflow with all of the required channels but without the two connected directories at both endpoints. Use this template and adapt it to your needs.

6.1.2.3.3. Example 3: Users with all Objects (Provisioning View Group)

Users are related to many other objects, such as privileges, business objects and other users. DirX Identity's predefined collection rule **Users with all objects** allows you to export this structure. You can find this collection rule in **Provisioning → Collections → Collections Rules → Default**. Check the **Content** tab for the definition, which is as follows:

- The first four definitions define the export of folders, as there are **countries, locations, organizations** and **organizational units** in the user tree.
- The next definition is the most complex one for the user object itself (**dxrUser**). It also

exports sub objects, the privilege assignment objects and defines a lot of links to other objects. Note that the links to other users define their own user entry definitions with level=1 and do not contain any further links to follow. This definition prevents loops from occurring and also prevents the entire user population from being exported starting from one single user object.

- The following definitions define all potential linked objects (**accounts, privileges, business objects** and **password policies**). These definitions are all set to level=1 and do not contain further link definitions.

The links to other users define their own user object definition with level=1 and do not contain any further links to follow. These definitions prevent loops from occurring and also prevent the entire user population from being exported starting from one single user object.

6.1.2.3.4. Example 4: Privilege Tree (Provisioning View Group)

In many cases, it makes sense to export a part of the privilege tree or the entire tree between systems, for example, from a development to a productive system. This type of export allows you to test new or extended privilege structures before releasing them to production. Use the predefined collection rule **Privilege tree** to export such structures. You can find this collection rule in **Provisioning → Collections → Collections Rules → Default**. Check the **Content** tab for the definition, which is as follows:

- This definition allows an export of containers (**dxrContainer**) with all their sub nodes.
- The next definition is for roles (**dxrRole**) and follows the links to junior roles (**dxrRoleLink**) and permissions (**dxrPermissionLink**).
- The permissions (**dxrPermission**) are now defined, which follow the links to groups (**dxrGroupLink**).
- The last definition is for target system groups (**dxrTargetSystemGroup**).

All of these definitions include all parents up to the highest level (the domain object). This definition ensures that no objects are missing at the target side. Note that each object is included only once into the collection.

This definition does not export the configuration of the target systems (the object descriptions etc.). You should set up separate collections to export these definitions; otherwise, DirX Identity cannot correctly display the account and group objects of a specific target system.

6.1.3. Exporting Data

DirX Identity provides a set of mechanisms to transport data from Connectivity and Provisioning databases. You can export these collections by hand or use a transport utility for more complex transfers and conversions.

The following export mechanisms are available:

Manual Collection Export - select one or more collection definitions in the tree pane, and

then select **Export Collection** from the context menu. This action exports all selected collections into separate files. For more information about this context menu selection, see "Common Context Menu Selections".

Manual Collection Folder Export - select a folder that contains collection definitions in the tree pane and then select **Export collections of subtree** from the context menu. This action exports all collection definitions from this subtree into separate files. For more information about this context menu selection, see "Common Context Menu Selections".

Manual Transport Export Workflow - define a transport export workflow that exports a set of collections. After loading the workflow to the Java-based Server, select **Run Workflow** from the context menu. The result is an export of all collection definitions into the corresponding files. For more information about this context menu selection, see "Common Context Menu Selections".

Scheduled Transport Export Workflow - define a transport export workflow that exports a set of collections. Set up a schedule that runs this workflow periodically. Load the workflow and the schedule to the Java-based Server. The result is an export of all collection definitions into the corresponding files at the defined time.

Batch Transport Export Workflow - set up an external batch script that defines a transport export. Run the script either by hand or scheduled (using your operating system's mechanism). The result is an export of all collection definitions into the corresponding files.

6.1.4. Deleting Data

You can use a collection definition to delete all entries the collection definition comprises. There are two ways of performing this operation:

- Use the **Delete Collection Entries** from the context menu of the collection (for details, see "Common Context Menu Selections"). After confirmation, all entries defined in this collection definition are removed from the database. Entries are only deleted if they would be also exported by the collection.
- Use the **Deletion** tab in a **Transport Import** workflow to define deletion of the previously imported objects before the new object set is imported. This method requires that the previously imported collections contain their collection definitions, or that there are collection definitions that permit deletion of the correct set of objects. You can use this deletion procedure to guarantee proper cleanup of a database before you import the new set of objects.

Don't use this deletion method if you have changed some of the previously imported objects by hand - for example, if you have modified some server addresses - because the deletion mechanism does not recognize these kinds of changes. Instead, define a more specific deletion procedure and an import procedure that does not change the manually-modified attribute values.

6.1.5. Importing Data

DirX Identity provides a set of mechanisms to transport data from Connectivity and Provisioning databases. You can import these collections by hand or use a transport utility for more complex transfers and conversions.

The following import mechanisms are available:

Manual Connectivity Collection Import - in the Expert View, right-click the root node of the **Connectivity** view group and then select **Import Data**. After you confirm the resulting dialog, a file selection dialog is displayed. Select the file to import. The meta controller imports the LDIF file and creates missing intermediate nodes automatically where necessary. Alternatively, you can use the **Import Collection File** method from the context menu of a collection object to import the previously exported collection file again. For more information about these context menu selections, see "Common Context Menu Selections".

Manual Provisioning Collection Import - select the root node of any of the views of the Provisioning view group. Select **File → Import** from the menu bar. Choose the file to import in the resulting file selection dialog. The file is imported. If intermediate nodes are missing, error messages are displayed. Check the export definition for a complete export definition and try the procedure again. Alternatively, you can use **Import Collection File** from the context menu of a collection object to import the previously exported collection file again. For more information about these context menu selections, see **"Common Context Menu Selections".**

Manual Transport Import Workflow - define a transport import workflow that imports a set of files. After loading the workflow to the Java-based Server, select **Run Workflow** from the context menu. The result is an import of all files into the target directory.

Scheduled Transport Import Workflow - define a transport import workflow that imports a set of files. Set up a schedule that runs this workflow periodically. Load the workflow and the schedule to the Java-based Server. The result is an import of all files into the target directory at the defined time.

Batch Transport Import Workflow - set up an external batch script that defines a transport import. Run the script either by hand or scheduled (using your operating system's mechanism). The result is an import of all collection definitions into the corresponding files.

6.1.6. Using Transport Workflows

Transport workflows allow the exchange of data from one directory to another. Data is exported from the source system into LDIF files and then imported from these files to the target system. This section provides information about import and export workflow setup and about Connectivity and Provisioning transport workflows.

6.1.6.1. Export Transport Workflow

An export transport workflow definition in the Connectivity view consists of the following items:

- Connection information to the source system, which consists of the address of the

source directory and the bind information.

- The data set to be exported, which consists of a set of predefined collections.
- If you want to create several files, use several collection definitions. Each collection can contain its own file name and path.
- If you intend to work with one file, define one collection (this collection defines the file name and path) and then include all other collections as sub collections.

We strongly recommend that you do not use Base64 format because it limits the ability to control and modify the input operation.

6.1.6.2. Import Transport Workflow

An import transport workflow definition in the Connectivity view consists of the following items:

- Connection information to the target system, which consists of the address of the target directory and the bind information.
- The data to be imported, which is defined as a set of files.
- A set of collections that allow for deletion and cleanup of the target database (optional).
- One or more domain mappings, if you handle Provisioning data and if source and target domains are different. If you import data from different domains, you can set up several domain mappings.
- One or more attribute mappings, as required. You can use all of the features of DirX Identity's framework for Java-based workflows, which include direct mapping (the default), constant mapping, simple expression mapping and Java-based mapping. Additional transport-specific features are delete, exclude and replace.

6.1.6.3. Connectivity Transport Workflows

This section describes some typical use cases of Connectivity transport workflows.

Transferring Workflows

In many cases, it is necessary to set up and test Java-based or Tcl-based workflows thoroughly in a development system before they are used in a production system. Keeping the trees synchronized is not easy. The following procedure (which describes Java-based workflows) can help to automate this process:

- Set up a rule-based collection in the development system that exports a set of Java-based workflows either with one common node or a set of common nodes. Use the **Java-based Workflows** sample collection rule to perform this task. This rule exports all related objects, including activities, ports and channels.
- Set up an export transport workflow that exports this collection from the development system to the associated file.
- Set up an import transport workflow that imports this file into the productive system.
- Define attribute mappings to create working applications, for example

- Set the active flag for all workflows to true with constant mapping
- Exchange cluster and resource definitions to the target values with constant or replace mapping

You can set up an export and import transport workflow in the opposite direction to transfer data from the production system to the development system.

We assumed only a development and a production system. Larger customer environments include an integration or test system between these two endpoints. In this case, you must set up workflows from the development to the integration system and then from the integration to the production system.

6.1.6.4. Provisioning Transport Workflows

This section describes some typical use cases of Provisioning transport workflows.

Exchanging Privilege Trees

In many cases, it is necessary to set up and test privilege hierarchies thoroughly in a development system before they are used in a production system. Keeping the trees synchronized is not an easy task. The following procedure can help to automate this process:

- Set up a rule-based collection in the development system that exports all roles starting either with one common node or a set of common nodes. Use the **Privilege tree** sample collection rule to perform this task. This rule exports also all inherited junior roles, all permissions and all groups of all target systems.
- Set up an export transport workflow that exports this collection from the development system to the associated file.
- Set up an import transport workflow that imports this file into the production system.
- In this case, we assume that the domain names are the same, so a domain mapping is not necessary.
- Because it is not desirable to transfer the group members, set up attribute mappings that exclude these attributes.

You can set up an export and import transport workflow in the opposite direction to transfer data from the production system to the development system.

We assumed only a development and a productive system. Larger customer environments include an integration or test system between these two endpoints. In this case, you must set up workflows from the development to the integration system and then from the integration to the production system.

Transferring User Trees

Use the following procedure to transfer a user subtree from one domain to another:

- Set up a rule-based collection in the source domain that exports all users starting either with one common node or a set of common nodes. Set up a collection rule that exports only the user objects: do not follow any links and do not transport the assignment objects under the user entries (set childLevel="1").
- Set up an export transport workflow that exports this collection from the source domain to the associated file.
- Set up an import transport workflow that imports this file into the target domain.
- Set up a domain mapping that converts the source domain to the target domain.
- Set up attribute mappings to guarantee that the user entries do not contain broken links. This step may require setting up exclude rules for the following attributes:
- Privileges: dxrGroupLink, dxrPermissionLink, dxrRoleLink, dxrInheritedPrivilegeLink, dxrPrivilegeLink
- Business Objects: dxrContextLink, dxrCostUnitLink, dxrLocationLink, dxrOrganizationLink, dxrOULink, dxrSecLocationLink, dxrSecOrganizationLink, dxrSecOULink
- Users: dxrRepresentative, manager, dxrSponsor, owner, secretary
- Password Policies: dxrPwdPolicyLink
- Note that you can keep some of these attributes if you are sure that the related objects exist. For example, if all managers and secretaries of these users are in the same tree, you can keep these attributes.
- To be sure that no broken links exist, use the link checker and let it remove broken links if necessary after the import of the data.

6.1.7. Running Transport Workflows in Batch Mode

You can run transport workflows as batch jobs. The following sections describe how to set up and configure such jobs. Set up an XML configuration file that defines options and use the corresponding batch script. Additionally / alternatively you can control the script via option switches. Run the script either by hand or scheduled (by means of your operating system).

You can set up jobs for

Export - produces a list of LDIF files based on collections defined in the Identity Store (both from Connectivity and Provisioning view groups) or deletes the entries in the LDAP directory.

Import - works with a list of LDIF files (for example produced from collections) that are joined using a set of mapping rules to the target Identity Domain.

6.1.7.1. Command Line

Both export and import jobs can run from a command line. The batch job files **exportConfig** and **importConfig** reside at the following location:

*install_path***tools\transport**

The general syntax of the command line is

jobname [**-conf** *filename*][*switches*] [*object* [*object* ...]]

where

jobname_
: is the name of the job, either **exportConfig** or **importConfig**.

***-conf* filename**
: defines an XML configuration file. The default is the built-in configuration file (see also the **printConf** parameter described later on in this section).

switches
: specifies a set of switches to control the job operation.

object
: is either an LDIF file path in case of an import or a collection DN in case of an export or delete.

The following switches are available:

-help or **-?** - displays help for this job (import or export)

-server *server* - specifies the LDAP server address (the default is "localhost")

-user *username* - specifies the LDAP user DN to connect to the server (the default is "cn=DomainAdmin,cn=My-Company")

-pwd *password* - specifies the LDAP user password (the default is "dirx")

-ssl true | false - specifies whether to use an SSL connection (the default is false)

-trace *tracefile* - specifies the trace file path (if not specified, no tracing is performed)

-level *level* - specifies the trace level (0-9, default is 0)

-delete - deletes the entries defined in the collections instead of exporting them. This switch is only available for **exportConfig**. For **importConfig** no corresponding switch is available.

-printXSD - displays the configuration XSD schema

-printConf - displays the default XML configuration (used when no configuration file is defined, see the **-conf** parameter described earlier in this section)

6.1.7.2. Export Configuration

Export manages exporting of collections based on given list of collection DNs or a search definition (search base and filter) or a combination of both.

Extra Command Line Switches

The following additional switches can override settings in the configuration file:

-searchBase *basenode* - the base node from which to search for collection definitions to process.

-filter *filter* - the filter (LDAP syntax) used to search for collections under the defined base node.

-base64 true | false - whether (true) or not (false) to encode exported collections in base64 (the default is false).

-maxLine *length* - the maximum line length in the exported LDIF file (important if a configuration management system has a restricted length). Use 2000 for ClearCase.

-**pageSize** *size* - the page size to use for internal one-level searches. A value of 0 means that paging is not used.

-delete - perform a delete operation instead of an export operation.

Selecting Collections

You can define the list of collections with a filter definition or with an explicit list of collection definitions.

You can specify the filter on the command line in LDAP notation or in the XML configuration file as a DSML filter definition. The **dxmObjectCollection** class is automatically added to the filter definition.

6.1.7.3. Import Configuration

Import manages the importing of LDIF files based on a given file list and provides custom mapping of attributes depending on various custom settings.

Extra Command Line Switches

The following additional switches can override settings in the configuration file:

-spml - indicates that input files are in SPML format

-srcDomain *srcdomain* - defines the source domain DN for domain mapping (for example, "cn=My-Company")

-tgtDomain *tgtdomain* - defines the target domain DN for domain mapping (for example, "cn=Customer Domain")

-attrFile *filename* - specifies the file to be used as the attribute source list. Otherwise the

attributes are read from the LDAP schema.

-simMode none | loggerSPML | simulateSPML | **loggerLDIF** | **simulateLDIF** - specifies the simulation mode:

loggerSPML - records the SPML request and modifies the target
simulateSPML - records the SPML request without any modifications in the target
loggerLDIF - records the request in **LDIF format** and modifies the target
simulateLDIF - records the request in **LDIF format** without any modifications in the target
none (default) - modifies the target without recording requests

-simFile *filename* - specifies the file to be used to record modifications. This switch is required when **simMode** is specified.

Standard Mapping Types

The Standard mapping types are as follows:

javaclass - use custom java class mapping

simpleexpression - use simple expression mapping

constant - use constant mapping

Transport-Specific Mapping Types

The transport-specific mapping types are as follows:

direct - set attribute value in the target from the value in the LDIF file

delete - delete all attribute values in the target

exclude - do not modify these attribute values

replace - replace patterns in attribute values

The patterns syntax is:

flags/*pattern*/*replacement*/

where

flags - specify occurrence and matching in the format

[*occurrence*][*matching*]

where

occurrence is either **a** (all occurrences, default) or **f** (first occurrence) and

matching is either **m** (case-sensitive, default) or **i** (case-insensitive).

If not specified the default value for *occurrence* is **a** (replace all occurrences of *pattern*) and

the default for *matching* is **m** (match case).

Examples:

- **f** - only the first occurrence of *pattern* is replaced, matching case.
- **i** - all occurrences of *pattern* are replaced, ignoring case.
- **ai** - all occurrences of *pattern* are replaced, ignoring case.

pattern - is a pattern definition in Java pattern syntax.

replacement - is a string with respect to character escaping (**$**, ****, **/** and so on).

Note that the characters ">" and "<" have a special meaning in XML and therefore they should be specified as **>** and **<**.

For a detailed description on Java Regular Expression syntax and examples see http://docs.oracle.com/javase/tutorial/essential/regex/.

Examples:

- All patterns (match case) of **search** are replaced with **replace**. The result for "I can search strings." is "I can replace strings."

a/search/replace/

- All words starting with multiple "a" are replaced by a single "a". The result for "aaaaargh aaron abele" is "argh aron abele".

i/\ba+([b-z][a-z]*)\b/a$1/

- All occurrences (ignore case) of "your<*anAdjective*>car" are replaced by "my<*theAdjective*>car. The result for "yourslowcar yourbluecar yourbluebike" is "myslowcar mybluecar yourbluebike".

im/your([a-z]*)car/my$1car/

Mapping Principles

There is an old way of mappings that are under <template> element in the XML configuration file and a new way mappings under <attrMapping> element. The GUI enables to edit/delete old way mappings and create/edit/delete new mappings.

Old Way Mapping

This attribute mapping allows specify only objectclass filter to match entries. **onemptyonly** and **oneaddonly** are handled as standalone mapping types. The old definitions are compatible with new functionality, but it is not recommended to create old way mappings in the GUI.

New Way Mapping

The new mapping offers a wider way of import possibilities. To use new approach, choose

the Attribute Config of type ExtendedAttributeDefinition. For each attribute, it is possible to select different mappings for different entries. The entries that match given conditions are mapped with given mapping type. Each attribute config can define multiple mapping choices in the configuration defined by the <mapitem> subelement in the GUI represented as a subnode of the attribute config node.

Each <mapitem> element has a <matching> section and mapping section. The matching section specifies conditions that must be met in order to use the mapping defined in mapping section. A condition could be an LDAP filter or a set of DN patterns or both. Conditions can also contain the following flags:

onemptyonly - use the mapping only if the value was not set and the joined entry exists.

onaddonly - use the mapping only for a new entry.

Remarks

See the XML schema of the configuration file or the online help to get a detailed description of the mapping elements.

6.1.8. Simulating Transport

The import transport feature allows you to simulate a run. Simulating an import transport can help you to determine:

- The changes that will be performed before you run the real import operation.
- Whether the source and target are synchronized

Simulation does not cover deletion of objects. Use procedure described in "Simulating Deletion" to check how deletion would be performed.

6.1.8.1. Simulating Import

This use case assumes that you want to check the import result before you really import it into the target.

Set the option **Simulation Mode** of your import workflow to **simulateLDIF**. Define a file name (for example, simulation.ldif) and a location for the simulation result.

Run the workflow. It generates two LDIF files that show the intended operations on the target.

The **simulation.req.LDIF** file contains all search requests for the target and the necessary add or modify operations. For example, for an add operation:

```
searchbase: cn=Customers,cn=B2B Roles,cn=RoleCatalogue,cn=Customer
Domain
scope: Base
```

```
dn: cn=Customers,cn=B2B Roles,cn=RoleCatalogue,cn=Customer Domain
changetype: add
objectClass: dxrContainer
objectClass: top
description: Roles for customers
dxrType: dxrRoleContainer
dxrUID: uid-7f001-6f26d110-11da5aeefcf--78dc
cn: Customers
```

For a modify operation:

```
searchbase: cn=RoleCatalogue,cn=Customer Domain
scope: Base

dn: cn=RoleCatalogue,cn=Customer Domain
changetype: modify
replace: description
description: Container for roles.
Setup your role tree here:
- Define a folder structure. You can use the structure either for
logical grouping of roles or for using such folders in access
policies.
- Create your roles in the defined structure.
- Assign permissions to these roles.
-
replace: dxrUID
dxrUID: metacp767f58-4a6078a8-7e3fc-358-a43c1-12d
-
```

The **simulation.rsp.LDIF** file contains all original records of the target and the necessary add or modify operation. For example, for an add operation:

```
dn: cn=Customers,cn=B2B Roles,cn=RoleCatalogue,cn=Customer Domain
changetype: add
objectClass: dxrContainer
objectClass: top
description: Roles for customers
dxrType: dxrRoleContainer
dxrUID: uid-7f001-6f26d110-11da5aeefcf--78dc
cn: Customers
```

For a modify operation:

```
dn: cn=RoleCatalogue,cn=Customer Domain
objectClass: dxrContainer
objectClass: top
cn: RoleCatalogue
description: Container for roles.
dxrUID: metacp767f58-4a60797c-8d00c-cf8-cc429-12d
dxrType: dxrRoleContainer

dn: cn=RoleCatalogue,cn=Customer Domain
changetype: modify
replace: description
description: Container for roles.
Setup your role tree here:
- Define a folder structure. You can use the structure either for
logical grouping of roles or for using such folders in access
policies.
- Create your roles in the defined structure.
- Assign permissions to these roles.
-
replace: dxrUID
dxrUID: metacp767f58-4a6078a8-7e3fc-358-a43c1-12d
-
```

If everything is as you expect it, set the option **Simulation Mode** of your import workflow to **loggerLDIF**. Define a file name (for example, logger.ldif) and a location for the logging result.

Run the workflow. It generates two LDIF files that show the real operations on the target (these operations should be identical to the simulation operations).

6.1.8.2. Comparing Systems

If two systems are synchronized, you would like to see what the differences are. Export the source system and then run a simulation against the target.

Set the option **Simulation Mode** of your import workflow to **simulateLDIF**. Define a file name (for example, compare.ldif) and a location for the simulation result.

Run the workflow. It generates two LDIF files that show the differences to the target.

You can see this information best in the **compare.req.ldif** file:

- It contains a lot of search requests. You can ignore them.

- Search for **changetype: modify** or **changetype:add** records. These records indicate the differences between source and target.

After reviewing the changes, you can set the Simulation Mode to loggerLDIF and synchronize the differences.

6.1.8.3. Simulating Deletion

Simulation does not cover deletion of objects. Use this procedure to check how deletion would be performed:

- Use the option "Export Collection" from the context menu of the related collections to be deleted. This action creates a backup file that contains all entries that shall be deleted. You can use this file to check which entries will be deleted before the import operation.
- Use the option "Delete Collection Entries" to find out if any conflicts occur, and then check into why these conflicts occur.
- Use the option "Import Collection File" to import the previously exported entries.

Now everything should be as it was before.

6.1.9. Hints and Warnings

Transporting data can cause some unwanted effects.Try to avoid them:

- **Transfer of Tcl-based workflows** - when objects that belong to Tcl-based workflow are updated during import operations, it can affect running workflows.For example, suppose that some activities are completed but others are still to be started.This situation can lead to inconsistencies because these activities use the updated information or a mix of original and updated information.
- **Transfer from older version to newer one** - do not import data from previous versions of DirX Identity.Important mandatory attributes could be missing, which results in strange behavior of the DirX Identity Manager.If you need to do this, two options exist:
  - in some cases, you can run a migration routine after importing the data
  - set up an import workflow that sets the missing mandatory attributes to fixed values.You can change them later on.
- **Transfer from newer version to older one** - if you want to transfer data from the current DirX Identity version to an older one, set up a batch import workflow that removes all attributes that did not exist in the previous DirX Identity version.Otherwise, you will encounter object class violations.

6.2. Using the Link Checker

The Link Checker searches for broken links in the Connectivity database or in a Provisioning domain, reports the broken links and optionally performs a cleanup.The check and cleanup functionality is configured by XML configuration files.

Four modes of operation are pre-configured:

- Check of a Provisioning domain
- Cleanup of a Provisioning domain
- Check of a Connectivity database
- Cleanup of a Connectivity database

You can change the behavior of the link checker via its configuration files.

Finally, this section provides information about Link Checker reports.

6.2.1. Checking a Provisioning Domain

To run a Provisioning domain check:

- Navigate to the folder *install_path*\GUI\tools\linkchecker
- You can check and adapt the configuration in the file **CheckProvisioningConfig.xml**. Read the link checker configuration file chapter for more information.
- Run the file **CheckProvisioning.bat**
- The results are reported in the files **CheckProvisioningTrace.txt** and **CheckProvisioningBroken.xls**

6.2.2. Cleaning Up a Provisioning Domain

To run a Provisioning domain cleanup operation:

we strongly recommend running a Provisioning domain check before you run the cleanup procedure.

- Navigate to the folder *install_path*\GUI\tools\linkchecker
- You can check and adapt the configuration in the file **CleanupProvisioningConfig.xml**. Read the link checker configuration file chapter for more information.
- Run the file **CleanupProvisioning.bat**
- The results are reported in the files **CleanupProvisioningTrace.txt** and **CleanupProvisioningBroken.xls**

6.2.3. Checking the Connectivity Database

To run a Connectivity database check:

- Navigate to the folder *install_path*\GUI\tools\linkchecker
- You can check and adapt the configuration in the file **CheckConnectivityConfig.xml**. Read the link checker configuration file chapter for more information.

- Run the file **CheckConnectivity.bat**
- The results are reported in the files **CheckConnectivityTrace.txt** and **CheckConnectivityBroken.xls**

6.2.4. Cleaning Up the Connectivity Database

To run a Connectivity domain cleanup:

- **Note:** we strongly recommend to run an Connectivity domain check before you run the cleanup procedure.
- Navigate to the folder *install_path***\GUI\tools\linkchecker**
- You can check and adapt the configuration in the file **CleanupConnectivityConfig.xml**. Read the link checker configuration file chapter for more information.
- Run the file **CleanupConnectivity.bat**
- The results are reported in the files **CleanupConnectivityTrace.txt** and **CleanupConnectivityBroken.xls**

6.2.5. Configuring the Link Checker

The configuration file controls the link checker's behavior.

Server Connection

user - the bind account.

password - the password for this account.

server - the host name of the LDAP server.

port - the port of the LDAP server.

ssl - whether (true) or not (false) to use SSL (the configuration is similar to the bind profile) The default is false.

domain - the root node where to start the check or cleanup.

Example:

```
<connection
user="cn=DomainAdmin,cn=My-Company"
password="dirx"
server="localhost"
port="389"
domain="cn=My-Company"
/>
```

Logging Configuration

fileName - the path and name of the trace file

level - the log level with a value range from 0 to 9. For a good readability of the report, use level="2".

Processing Mode

The mode is configured in the process tag:

process mode - defines the processing mode. Supported values are:*
check* - in this mode broken links are checked but not modified.*
cleanup* - in this mode broken links are reported and removed.

You can overwrite this mode for single object classes.

Object Types and Link Attributes

The object classes of the objects to be checked and its link attributes are defined in the linkdef tag, having the attributes objectClass and "attributes" and (optionally) mode.

For each linkdef definition, one simple paged search is performed, returning all objects of the specified object class. For each object, the link attributes to be checked are read from the comma-separated attributes in the linkdef tag.

Example:

<linkdef objectClass="dxrRole" attributes="dxrRoleLink,dxrPermissionLink" mode="check" />

In this example, all roles are processed. For each role, the contents of dxrRoleLink and dxrPermissionLink is checked. In case "mode" is defined in a linkdef tag, it overwrites the global default value from the processing mode section.

Unreferenced Map Items in the Connectivity Database

mapitems - a specialized routine checks or cleans unreferenced map items in the Connectivity database. Supported values are:*
none* - does not check for broken map items (this is the default mode if the complete tag is missing)*
check* - checks for broken map items
cleanup - performs a cleanup of broken map items

6.2.6. Link Checker Reports

The Link Checker generates a report as shown below.

```
LOG(LNC201): Program 'Link Checker', Version '1.0.0.0' of '2004-11-
16' started ***
```

```
LOG(LNC100):
------------------------------------------------------------------------
-----------
ERR(LNC406): User                                          | link
attribute | broken link (cleanup)
ERR(LNC406): cn=DomainAdmin                                | RoleLink
| cn=test,cn=RoleQAPSr,cn=QA,cn=RoleCatalogue,cn=My-Company
ERR(LNC406): cn=DomainAdmin                                |
PermissionLink | cn=broken,cn=Permissions,cn=root
ERR(LNC406): cn=FOSTER HAROLD,ou=METAROLE,cn=Users         | RoleLink
| cn=test,cn=RoleQAPSr,cn=QA,cn=RoleCatalogue,cn=My-Company
ERR(LNC406): cn=FOSTER HAROLD,ou=METAROLE,cn=Users         |
PermissionLink | cn=broken,cn=Permissions,cn=root
ERR(LNC406): cn=RAYMOND ALEXANDER,ou=METAROLE,cn=Users     | RoleLink
| cn=test,cn=RoleQAPSr,cn=QA,cn=RoleCatalogue,cn=My-Company
ERR(LNC406): cn=RAYMOND ALEXANDER,ou=METAROLE,cn=Users     |
PermissionLink | cn=broken,cn=Permissions,cn=root
ERR(LNC406): cn=CANIFF MILTON,ou=METAROLE,cn=Users         | RoleLink
| cn=test,cn=RoleQAPSr,cn=QA,cn=RoleCatalogue,cn=My-Company
ERR(LNC406): cn=CANIFF MILTON,ou=METAROLE,cn=Users         |
PermissionLink | cn=broken,cn=Permissions,cn=root
ERR(LNC406): cn=HOGARTH BURNE,ou=METAROLE,cn=Users         | RoleLink
| cn=test,cn=RoleQAPSr,cn=QA,cn=RoleCatalogue,cn=My-Company
ERR(LNC406): cn=HOGARTH BURNE,ou=METAROLE,cn=Users         |
PermissionLink | cn=broken,cn=Permissions,cn=root
ERR(LNC406): cn=TUFTS WARREN,ou=METAROLE,cn=Users          | RoleLink
| cn=test,cn=RoleQAPSr,cn=QA,cn=RoleCatalogue,cn=My-Company
ERR(LNC406): cn=TUFTS WARREN,ou=METAROLE,cn=Users          |
PermissionLink | cn=broken,cn=Permissions,cn=root
ERR(LNC406): cn=MCCAY WINSOR,ou=METAROLE,cn=Users          | RoleLink
| cn=test,cn=RoleQAPSr,cn=QA,cn=RoleCatalogue,cn=My-Company
ERR(LNC406): cn=MCCAY WINSOR,ou=METAROLE,cn=Users          |
PermissionLink | cn=broken,cn=Permissions,cn=root
ERR(LNC406): cn=HERRIMAN GEORGE,ou=METAROLE,cn=Users       | RoleLink
| cn=test,cn=RoleQAPSr,cn=QA,cn=RoleCatalogue,cn=My-Company
ERR(LNC406): cn=HERRIMAN GEORGE,ou=METAROLE,cn=Users       |
PermissionLink | cn=broken,cn=Permissions,cn=root
ERR(LNC406): cn=MCMANUS GEORGE,ou=METAROLE,cn=Users        | RoleLink
| cn=test,cn=RoleQAPSr,cn=QA,cn=RoleCatalogue,cn=My-Company
ERR(LNC406): cn=MCMANUS GEORGE,ou=METAROLE,cn=Users        |
PermissionLink | cn=broken,cn=Permissions,cn=root
```

```
ERR(LNC406): cn=KNERR HAROLD,ou=METAROLE,cn=Users        | RoleLink
| cn=test,cn=RoleQAPSr,cn=QA,cn=RoleCatalogue,cn=My-Company
ERR(LNC406): cn=KNERR HAROLD,ou=METAROLE,cn=Users        |
PermissionLink | cn=broken,cn=Permissions,cn=root
ERR(LNC406): cn=SEGAR ELZIE CRYSLER,ou=METAROLE,cn=Users | RoleLink
| cn=test,cn=RoleQAPSr,cn=QA,cn=RoleCatalogue,cn=My-Company
ERR(LNC406): cn=SEGAR ELZIE CRYSLER,ou=METAROLE,cn=Users |
PermissionLink | cn=broken,cn=Permissions,cn=root
ERR(LNC406): cn=tttt,cn=Users                            | RoleLink
| cn=test,cn=RoleQAPSr,cn=QA,cn=RoleCatalogue,cn=My-Company
ERR(LNC406): cn=tttt,cn=Users                            |
PermissionLink | cn=broken,cn=Permissions,cn=root
ERR(LNC406): UserToPermission                            | link
attribute | broken link (check)
ERR(LNC406): cn=uid...,cn=tttt,cn=Users                  | AssignFrom
| cn=tttt broken,cn=Users,cn=My-Company
ERR(LNC406): UserToGroup                                 | link
attribute | broken link (check)
ERR(LNC406): cn=uid...,cn=tttt,cn=Users                  | AssignFrom
| cn=tttt broken,cn=Users,cn=My-Company
ERR(LNC406): cn=uid...,cn=tttt,cn=Users                  | AssignTo
| cn=QAUsers
broken,cn=Groups,cn=Exchange5.5DL,cn=TargetSystems,cn=My-Company
LOG(LNC100):
-------------------------------------------------------------------
-----------
LOG(LNC202): Program 'Link Agent' ended with 0 fatalError(s), 30
error(s), and 0 warning(s).
```

The broken links are reported in a table with three columns.

If there are broken links for an objectClass, a header row is written, with objectClass without "dxr/dxm" prefix, "link attribute" and broken link (cleanup) or broken link (check), depending on the mode configured.

This header row is followed by data rows, one for each broken link.The first column contains the dn of the object.To save space, the domain root is removed from the distinguished name (DN).The second column contains the link attribute without the "dxr/dxm" prefix.The third column contains the value of the broken link.

6.3. Using the Log Analyzer

Use the log analyzer tool (**logAnt**) to analyze complex Java-based Server log files.The tool

solves two issues:

- It writes for each workflow instance a separate file that comprises all log entries and messages.Now you have two views on Java-based Server operation: the original log files show the operation sequence as a long list of messages.The separated files allow you to view specific workflow instances.Both views are necessary for analysis of run-time behavior and in case of problems.
- It writes statistics files in CSV format that list each workflow instance as one line.Use Microsoft Excel to analyze such files.This allows you to get an overview for a specific time range of Java-based Server operation.

Request workflows can now run several Java-based Servers.As a result, several log files must be evaluated in order to get a complete overview of one workflow.If you are running several Java-based Servers, you must evaluate all log files (using **logANT**) and use the log merging tool (**logMerge**) that generates one file per workflow but merges all logs of the different Java-based Servers based on the time stamps.

If you are running the Java-based Servers in a heterogeneous environment (Windows, UNIX), you should run **logANT** both on your Windows and UNIX machines because the log files normally use a different time stamp format in the log files.Next, copy the output files of **logANT** to any of the machines and then run **logMerge**.

If all your Java-based Servers run in a homogeneous environment (producing the same time stamp format in the log files), you can copy the server log files on one machine (using one folder per Java-based Server) and then run **logANT** and then **logMerge**.

The next sections explain:

- How to configure and use the log analyzer tool (logAnt)
- How to work with the separated files
- How to analyze statistics files

6.3.1. How to Use Log Analyzer

The log analyzer tool **logAnt** reads the Java-based Server log files (server*.txt) and creates separated workflow-specific files as well as statistics files.

The files are written into a configurable status area, grouped by folders *workflow name*.

The file names are built from the start time and the workflow instance id, for example

20100528_050302.781_128dcd9f7361086.log

Note that the dollar signs ($) in the UID are removed to avoid problems with UNIX file names.

In addition, a statistics file is written in CSV format that provides an overview of all workflow runs.

6.3.1.1. Configuring the Log Analyzer

Use the **logANT.ini** file to configure the tool.

Input and Output

inputPath - pathname(s) of the logs folder that contains the Java-based Server log files to be analyzed. The **inputPath** is a comma-separated list of pathnames where the log file folders of the different Java-based Servers need to be listed. If the Java-based Servers run on different platforms, then you need to copy the log files manually to a new subfolder (one new subfolder per remote Java-based Server) on your local computer.
Example: sampleData/logs
sampleData1/logs,sampleData2/logs,sampleData3/logs

outputPath - pathname(s) of the folder where to store the analyzed files. The **outputPath** is a comma-separated list of folder names (one folder per Java-based Server).
Example: sampleData/status
sampleData1/status,sampleData2/status,sampleData3/status

statisticsFileName - pathname(s) of the statistics file. The **statisticsFileName** is a comma-separated list of statistics files (one statistics file per Java-based Server).
Example: sampleData/status/statistics.csv
sampleData1/status/statistics.csv,sampleData2/status/statistics.csv,
sampleData3/status/statistics.csv

The number of pathnames in **inputPath**, **outputPath** and **statisticsFileName** must be same for all three parameters.

Format and Filtering

completeOnly - set this flag to true if you want to suppress incomplete log files. Otherwise, (if set to false) all log files are extracted, even incomplete ones where the beginning or the end is missing.

dateFormat - the date format string. The following 2 formats are automatically selected as defaults:
dd.MM.yyyy HH:mm:ss.SSS
MMM dd, yyyy HH:mm:ss.SSS

Define your own date format if those formats do not apply. See SimpleDateFormat javadoc for format definitions

filterPath - a partial path describing one or more workflows that have to be analyzed.
All workflows under the filterPath are processed. If empty, all workflows are considered.
Examples:
My-Company/Main/Identity Store/ → delivers all real-time maintenance workflow instances of the My-Company folder
Definitions/My-Company → extracts all request workflow instances of the My-Company sub-folder

filterID - a (partial) workflow instance ID defining one (or more) special workflow(s) to be

analyzed.
Example: 128f3a4e274$-758a
Note: if you copy these IDs from a file name, be aware that the $ was removed!

Trace Configuration

trace.filename - the name of the trace file.
Example: sampleData/logANT.trc

trace.level - the trace debug log level for the output to the trace file. Allowed values are 0 to 9. No file is written if trace.level is set to 0.

console.level - the console debug log level for the output to the trace file. Allowed values are 0 to 9. No console output is written if trace.level is set to 0.

6.3.2. How to Use Separated Files

The log analyzer writes a set of files into a flat folder structure under the **outputPath** where the folder names are workflow names, for example:

EventBasedAccountProcessing
EventBasedUserResolution
PasswordEventManager

Each file in such a folder represents a workflow instance. The file extension informs you about specific situations

.log - a complete file with no errors and warnings.

.err - a complete file with errors (and maybe warnings).

.war - a complete file with warnings only.

.inc_log - an incomplete file with no errors and warnings.

.inc_err - an incomplete file with errors (and maybe warnings).

.inc_war - an incomplete file with warnings only.

Because you analyze typically only a set of log files that represent a specific time range some of the files might be incomplete. This is indicated by a file extension that starts with **inc**.

Analysis of a Workflow Instance File

Workflow instance files contain all messages that belong to a specific workflow instance. Java-based Server log file lines in the original log files can be very long and thus hard to interpret.

A typical file has this structure:

Line 1: *start_time* [*thread*] [*workflowPath*], for example:

Jun 30, 2010 13:41:26.480 [colocated-0] [My-Company/Main/Identity Store/EventBasedAccountProcessing/12988a86e5f$-3a5a]_
start_time_ - the time where this workflow instance was started._
thread_ - the first thread who worked on that workflow._
workflowPath_ - the workflow path of the instance. This path is valid for the whole file.

Line and following lines: *timestamp* [*threadShortcut*] *message*, for example:
13:41:26.480 [c-0] [initiator=ResolveTask] wfID [uid=12988a86e5f$-3a23, expired=false]: WF start_
timestamp_ - a time stamp without date when this message occurred._
thread_ - either a complete thread specification (a TCP IP address) or a shortcut. c-*n* stands for 'colocated-*n*'._
message_ - the message itself.

For realtime workflows, all following messages have a standardized format. For request workflows, there are different message types:

- Messages which contain a workflow path and a workflow ID. These messages have the same standardized format as for realtime workflows.
- Messages of the Java-based Server extension for request workflows (REQWF):
- Messages representing internal handling of a request workflow instance and which contain the workflow ID only. These messages contain timestamp, thread and the message text itself.
- Messages representing a request workflow instance start without even a workflow ID. These messages contain timestamp, thread and the message text itself.

See the samples below for a better understanding.

Realtime Workflow File Sample

Here is an example file (with preceded line numbers for reference):

```
Jun 30, 2010 13:41:26.480 [colocated-0] [ My-Company/Main/Identity

Store/EventBasedAccountProcessing/12988a86e5f$-3a5a ] ①
13:41:26.480 [c-0] [initiator=ResolveTask] wfID [uid=12988a86e5f$-

3a23, expired=false]: WF start ②
13:41:26.481 [c-0] IDSJ654 State of workflow with ID '12988a86e5f$-

3a5a' (12988a86e5f$-3a5a) changes from '' to 'RUNNING'. ③
13:41:26.481 [c-0] IDSJ651 State of activity 'join' of workflow with
ID '12988a86e5f$-3a5a' (12988a86e5f$-3a5a) changes from 'PREPARING'

to 'RUNNING'. ④
13:41:26.531 [c-5] [join,initiator=.] EBR001 AccountEventController

received ModifyEvent with id = ... ⑤
```

```
 13:41:26.729 [c-5] EBR039 AccountEventController finished processing
a ModifyEvent for Entry ... ⑥
...
13:41:26.898 [c-5] IDSJ651 State of activity 'join' of workflow with
ID '12988a86e5f$-3a5a' (12988a86e5f$-3a5a) changes from 'RUNNING' to
'SUCCEEDED'. ⑦
13:41:26.898 [c-5] IDSJ659 State of activity 'join' of workflow with
ID '12988a86e5f$-3a5a' changes to 'SUCCEEDED'. Workflow put to Java
space. ⑧
13:41:26.904 [c-0] [initiator=join] IDSJ651 State of activity 'join'
of workflow with ID '12988a86e5f$-3a5a' (12988a86e5f$-3a5a) changes
from 'RUNNING' to 'SUCCEEDED'. ⑨
13:41:26.913 [c-0] IDSJ654 State of workflow with ID '12988a86e5f$-
3a5a' (12988a86e5f$-3a5a) changes from 'RUNNING' to 'SUCCEEDED'. ⑩
```

① The first message contains the start time and the full workflow path.

② This line shows a workflow start message that was produced by the thread **colocated-0** which runs in the Java-based Server itself. This thread represents the workflow engine.

③

④ The workflow engine (c-0 = colocated-0) changes the workflow instance state to RUNNING and the activity state to RUNNING and puts the workflow item into the Java space where threads for this resource family (not visible here) can lease and work on it.

⑤

⑥ A specific thread (c-5 = colocated-5) leased this workflow item from Java space and works on it. The messages here are individual to the workflow type.

⑦

⑧ These two lines show the end of the work for thread colocated-5. It puts the Workflow back to Java space.

⑨

⑩ The workflow engine (colocated-0) takes over and finishes this workflow instance.

This is a sample of a workflow that is processed in one step, which means that the workflow engine prepares the workflow and then it is processed by a specific thread. If workflow runs in steps or if an error activity is triggered, the workflow engine puts the workflow several times to Java space and there may be different specific threads that work on this workflow instance.

Request Workflow File Sample

Here is an example file (with preceded line numbers for reference). Messages of the Java-based Server extension for request workflows are shown in bold type:

```
29.04.2015 09:15:28.050 [http-nio-40000-exec-1] [
confdb/workflows/Definitions/My-Company/Approval/4-Eye

Approval/14d04020c7a$-7a0e ] ①
09:15:28.050 [http-nio-40000-exec-1] [] REQWF307
"createWorkflowInstance" started; authenticated user:

cn=DomainAdmin,cn=My-Company, workflowName: null, language: null. ②
09:15:29.095 [http-nio-40000-exec-1] REQWF308
"createWorkflowInstance" of workflowID '14d04020c7a$-7a0e' terminated

successfully. ③
09:15:29.157 [c-1] [initiator=Service (WorkflowServiceImpl)] IDSJ676
Running Workflow {uid=14d04020c7a$-7a0e,
repositoryID=cn=14d04020c7a$-7a0e,cn=2015-04-29,cn=4-Eye
Approval,cn=Approval,cn=My-Company,cn=monitor,cn=wfroot,cn=My-
Company, properties=null,
{resourcefamily={workflowengine}}initiator=Service

(WorkflowServiceImpl)}. ④
09:15:29.204 [c-1] IDSJ657 State of activity 'Approval by Privilege
Managers' of workflow with ID '14d04020c7a$-7a0e' (My-
Company/Approval/4-Eye Approval/2015-04-29/Pitton Lavina -> Analyst

Reports) changes from 'null' to 'null'. Workflow put to Java space. ⑤
09:15:29.251 [c-1] IDSJ657 State of activity 'Approval by User
Manager' of workflow with ID '14d04020c7a$-7a0e' (My-
Company/Approval/4-Eye Approval/2015-04-29/Pitton Lavina -> Analyst

Reports) changes from 'null' to 'null'. Workflow put to Java space. ⑥
09:15:29.251 [c-1] IDSJ650 State of activity 'Approval by User
Manager' of workflow with ID '14d04020c7a$-7a0e' (My-
Company/Approval/4-Eye Approval/2015-04-29/Pitton Lavina -> Analyst

Reports) changes from 'PREPARING' to 'RUNNING'. ⑦
…
09:16:13.347 [http-nio-40000-exec-2] REQWF319 "getWorkflowInstance"
started; authenticated user: cn=Benetton
Gianfranco,ou=Marketing,o=My-Company,cn=Users,cn=My-Company,
workflowID: '14d04020c7a$-7a0e', language: de.
```

```
09:16:13.427 [http-nio-40000-exec-2] REQWF320 "getWorkflowInstance"
of workflowID '14d04020c7a$-7a0e' terminated successfully.
…
09:16:17.300 [c-1] IDSJ650 State of activity 'Apply Approved
Privilege Change' of workflow with ID '14d04020c7a$-7a0e' (My-
Company/Approval/4-Eye Approval/2015-04-29/Pitton Lavina -> Analyst

Reports) changes from 'RUNNING' to 'SUCCEEDED'. ⑧
09:16:17.300 [c-1] IDSJ653 State of workflow with ID '14d04020c7a$-
7a0e' (My-Company/Approval/4-Eye Approval/2015-04-29/Pitton Lavina ->

Analyst Reports) changes from 'RUNNING' to 'SUCCEEDED'. ⑨
09:16:17.456 [c-1] IDSJ660  Workflow 14d04020c7a$-7a0e ('My-
Company/Approval/4-Eye Approval/2015-04-29/Pitton Lavina -> Analyst

Reports') has finished. Cleanup started. ⑩
09:16:17.549 [http-nio-40000-exec-2] [] REQWF354 "waitForIdle" of

workflowID '14d04020c7a$-7a0e' terminated successfully. ⑪
```

① The first message contains the start time and the full workflow path.

② This line shows the start of a **createWorkflowInstance** operation initiated by the Request Workflow processor. The workflow path and the workflow ID are not yet known at operation start.

③ This line shows successful termination **createWorkflowInstance** operation including the resulting workflow ID.

④ This line shows a workflow start message that was produced by the thread **colocated-1** which runs in the Java-based Server itself. This thread represents the workflow engine.

⑤

⑥

⑦ The workflow engine (c-1 = colocated-0) changes the workflow instance state to RUNNING and the activity state to RUNNING and puts the workflow item into the Java space where threads for this resource family (not visible here) can lease and work on it.

⑧

⑨

⑩ The workflow engine (colocated-1) takes over and finishes this workflow instance.

⑪ The operation **waitForIdle** terminated successfully.

This is a sample of a request workflow where all relevant approvers accepted an assignment of a privilege to a user.

6.3.3. How to Use Statistics Files

The log analyzer writes statistics files in CSV format that comprise not more than 65535 lines. This limit comes from Microsoft Excel that does not allow more lines.

Each workflow instance is represented by one line in such a file. The next sections explain the statistics file format and elaborate how to analyze such a file.

6.3.3.1. Statistics File Format

The statistics file contains a header line with the field names and then up to 65535 lines with these fields:

Start time - the date and time when the workflow started or when the analysis started (if the workflow start is not contained in the file).

End time - the date and the time when the workflow ended or when the analysis ended (if the workflow end is not contained in the file).

Duration - the duration of this workflow run in the format hh:mm:ss,000 (the last three digits represent milliseconds).

Wf-Name - the name of the workflow (without the path, see below).

Wf-ID - the workflow ID. This field is important for backtracking into the original log files.

Complete - a flag that indicates that the workflow was completely processed (no missing lines at the beginning or at the end). The following values can occur:*
C* - complete
I - start or end missing

ERR - the number of error messages that occurred within this workflow run.

WAR - the number of warning messages that occurred within this workflow run.

Path - the complete workflow path

Example:

Jun 30, 2010 13:32:58.995;Jun 30, 2010 13:33:04.197;00:00:05.202;SetPassword in Intranet;129889a4697$5b48;C;0;0;My-Company/Main/Target Realtime/Intranet Portal

6.3.3.2. How to Analyze Statistics Files

You can analyze the resulting statistics files best with Microsoft Excel. Perform the following steps to analyze a file with the delivered analysis template.

Preparing the Analysis

Perform these steps:

- Be sure that Microsoft Excel is installed on the machine where you want to analyze the

statistics file.

- Copy the file **statistics_template.xls** from the product media.
- Copy it to **statistics.xls** or any other file name.
- Open the statistics file (let's assume its name is **output.csv**) that was produced by the log analyzer tool (double click it). Excel should display a page with the data already separated to columns. If this is not the case, use the Data → Import External Data function of Excel to read the input correctly.
- Open the prepared **statistics.xls** file.
- Select the **Data** tab. It should be empty.
- Copy and paste all lines from the opened **output.csv** file to the Data tab into cell A1. You can now close the output.csv file (do not save it) because we do not need it anymore.
- Perform **Tools → Macro → Macros** and run the macro **Statistics_Format**

Viewing Statistics

In this section you can view statistics on all entered data. Perform these steps:

- Click the **Workflows** tab and then select a cell in the pivot table.
- Perform **Refresh Data** from the context menu.
- The table shows now statistics on the data coming in the **Data** tab.

For each workflow name you can see:

Count - the number of workflow runs found.

Minimum of Duration - the minimum duration of all these workflow runs.

Average of Duration - the average duration of all these workflow runs.

Maximum of Duration - the maximum duration of all these workflow runs.

Sum of Errors - the sum of all error messages for this workflow type.

Sum of Warnings - the sum of all warning messages for this workflow type.

Additionally, you can view the last three parameters in graphical form:

- Perform the same action on the **Table** tab to refresh the chart in the **Chart** tab.
- Click the **Table** tab and then select a cell in the pivot table.
- Perform **Refresh Data** from the context menu.
- Click the Chart tab.

The chart shows now statistics on the data in the **Data** tab in graphical form.

Viewing Workflow Runs Over Time

Here you can view the behavior of all workflow runs over time.

- Lookup the last line in the Data tab.Let's assume it is for example 1447.
- Click the **Timing** tab and click in the middle of the chart.
- Perform **Source Data** from the context menu and then click the **Series** tab.
- Click the All workflows series and enter '=Data!C2:C1447' into the **Values** field.Enter '=Data!A2:A1447' into the **Category (X) axis labels** field.Click OK.

The chart displays the duration of all workflow runs (y-axis) over the parameter start time (x-axis).You can easily see if there are hot spots or areas where workflows need a longer time.

6.4. Using the Log Merger

Use the Log Merger (**logMerge**) if you are running several Java-based Servers and you want to merge workflow-specific log files that have been generated (using the **logANT** tool).

The Log Merger processes all the output folders that have been generated by **logANT** and then generates one file per workflow.The merging of the records is performed on the time stamps.

The Log Merger solves two issues (same as in **logANT**, but for all output files of **logANT**):

- It writes a separate file for each workflow instance that comprises all log entries and messages.Now you have two views on Java-based Server operation: the original log files show the operation sequence as a long list of messages.The separated files allow you to view specific workflow instances.Both views are necessary for analysis of run-time behavior and in case of problems.
- It writes statistics files in CSV format that list each workflow instance as one line.Use Microsoft Excel to analyze these files.This technique allows you to obtain an overview of a specific time range of Java-based Server operation.

The next sections explain:

- How to configure and use the Log Merger (**logMerge**)
- How to work with the separated files
- How to analyze statistics files

6.4.1. How to Use the Log Merger

The Log Merger (**logMerge**) reads the output files generated by **logANT** and creates separate workflow-specific files and statistics files.

The files are written into a configurable status area, grouped by folders workflow name.

The file names are built from the start time and the workflow instance ID, for example:

```
20100528_050302.781_128dcd9f7361086.log
```

The dollar signs ($) in the UID are removed to avoid problems with UNIX file

> names.

A statistics file is also written in CSV format that provides an overview of all workflow runs.

6.4.1.1. Configuring the Log Merger

Use the **logMerge.ini** file to configure the tool.

6.4.1.2. Input and Output

inputPath - pathname(s) of the logs folder that contains the workflow-specific log files to be merged. The **inputPath** is a comma-separated list of pathnames where the workflow-specific log files have been generated by a previous call to **logANT**.

Example: sampleData/status
sampleData1/status,sampleData2/status,sampleData3/status

outputPath - pathname of the folder in which to store the merged files.

Example: sampleData/status

statisticsFileName - pathname of the overall statistics file.

Example: sampleData/status/statistics.csv

6.4.1.3. Trace Configuration

trace.filename - the name of the trace file.

Example: sampleData/logMerge.trc

trace.level - the trace debug log level for the output to the trace file. Allowed values are 0 to 9. No file is written if **trace.level** is set to **0**.

console.level - the console debug log level for the output to the trace file. Allowed values are 0 to 9. No console output is written if **trace.level** is set to **0**.

6.4.2. How to Use Separated Files

The Log Merger writes a set of files into a flat folder structure under the **outputPath** where the folder names are workflow names.

The same information applies as for **logANT**, as **logMerge** just creates an overall view of the workflow-specific logs.For more details, see "How to Use Separated Files" in the section "Using the Log Analyzer".

6.4.3. How to Use Statistics Files

The Log Merger writes an overall statistics files in CSV format that comprises no more than 65535 lines.This limit comes from Microsoft Excel, which does not allow more lines.

Each workflow instance is represented by one line in the file.

The same information applies as for logANT, as logMerge just creates an overall view of the workflow-specific logs.For more details, see the section "How to Use Statistics Files" in the section "Using the Log Analyzer".

6.5. Using the Log Viewer

Use the Log Viewer (**logViewer**) tool to analyze complex Web Center log files.The tool solves two issues:

It displays all requests (Struts actions) within that log file in a list.

For each request you can open a details window that displays the complete logging part of this request.

The next sections explain:

- How to use the Log Viewer (logViewer) tool
- How to work with the request list
- How to work with the details window

6.5.1. How to Use the Log Viewer

The log analyzer tool **logViewer** reads Web Center debug log files (usually **stdout.***timestamp***.txt** in the folder *TOMCAT_HOME***\logs**) and prepares them for detailed analysis.

The log files must be obtained with Web Center log level set to DEBUG. (Assign the value **2** to the parameter **com.siemens.webMgr.log.level** in Web Center's **web.xml**.)

6.5.1.1. Configuring the Log Viewer

There are currently no configuration options.

6.5.1.2. Running the Log Viewer

Perform these steps:

- Unpack the tool to any folder you like.
- Copy a Web Center debug log file to the **logViewer\log** folder.
- Rename it to **log.txt**.
- Run the **logViewer\run.bat** (or the **logViewer/run.sh**) file.
- After a few seconds the result is created in the log folder.
- Start the **logViewer\log\summary.html** page. The tool displays all requests (Struts actions) in a list. (Use the tool tips to understand the columns and items.)
- Clicking a row opens a separate window that displays the complete logging part for this

specific request.

6.5.2. How to Use the Request List

The request list displays all requests as a list. The meaning of the columns is:

R - the request sequence number.

Start - start time for this request.

End - end time for this request.

Time - duration of this request.

Session ID - the identifier of the session. The tooltip displays the full session id. A flag indicates whether the session was newly created (**N**) or already in use before (**U**).

SSL ID - the SSL identifier for requests sent via HTTPS.

Loginname - the common name of the logged-in user. The tooltip displays the user's full DN.

SSO User - the single sign-on username in case of a single sign-on request.

Path - the requested Struts action. The tooltip displays also the JSP executed and the form bean name. The special paths **STARTUP** and **SHUTDOWN** indicate that the Web Center application was started and stopped, respectively.

Forward - the action forward returned from the executed JSP.

Target - the path assigned to the action forward. The path is either a Struts action or a Tiles definition name. In case of a Struts action, a flag indicates whether the action is invoked via an HTTP redirect (**R**) or via a local redirection (**L**).

Exceptions - any exceptions that occurred during request processing.

Use the scroll bars to navigate within the list.

6.5.3. How to Use the Details Window

This window shows all messages for a specific request. The top level line allows navigation through the request list:

(name) - the request name in the form **r***n*-**s***n*-*action* where
r*n* - indicates the sequence request number
s*n* - indicates the sequence session number. **s0** is displayed for start and stop requests.
action - defines the Struts action.

Fix session - use this flag to fix the current session. This allows navigating only within the request list of this session. In the rest of this chapter, first (next, previous, last) request means the first (next, previous, last) request in the current session if this flag is enabled.

First - displays the first request in the list.

Startup - displays the most recent previous the startup request.

Exc - displays the most recent previous request that threw an exception.

Prev - displays the previous request in the list.

Next - displays the next request in the list.

Exc - displays the next request that threw an exception.

Shutdown - displays the next shutdown request.

Last - displays the last request in the list.

Use the scroll bars to navigate in the message list.

6.6. Using the Run Workflow Tool

The run workflow tool allows you to start workflows from any location inside the network from the shell level.The tool is Java-based and can run on all DirX Identity supported platforms.The tool does not need any other parts of the DirX Identity system installed.You can use it to start workflows triggered by any event outside DirX Identity (event trigger).

The run workflow tool consists of two components to run workflows in the C++-based Server and in the Java-based Server.

The functionality to execute a workflow is provided as two Java classes (**siemens.dxm.tools.RunWorkflow** for a workflow running in the C++-based Server and **siemens.dxm.tools.RunJavaWorkflow** for a workflow running in the Java-based Server), the delivered batch files act as wrappers.The tool connects to the configuration database (via LDAP) and reads the bind credentials to establish a connection to the DirX messaging service.If this action succeeds, subsequent messages are sent to the appropriate C++-based Server to start and monitor the workflow.For workflows running in the Java-based Server, one message is sent to the messaging system that triggers the workflow; the workflow itself is not monitored by the run workflow tool.

6.6.1. Installing the Run Workflow Tool

Note: All machines where DirX Identity is installed already contain an installed version of the run workflow tool.Extra installation is not necessary.On all other machines, perform this sequence:

- The Java Runtime Environment (JRE) must be installed on the machine. (See the readme file on the DVD for the version supported.)
- A zip or tar file is delivered with DirX Identity in the folder: *install_path***tools\utilities\runwf.zip** (on Windows) or *install_path***tools\utilities\runwf.tar** (on Linux)
- Extract the file **runwf.zip** to any file directory of your choice on Windows platforms.

- Unpack the file **runwf.tar.gz** (using gunzip and tar) into any file system directory on UNIX platforms. Perform **chmod 755 runwf.sh**.

6.6.2. Running the Run Workflow Tool

For workflows running in the C++-based Server, you can run the tool with one of the commands:

- **runwf.bat** *workflow-path* (on Windows)
- **runwf.sh** *workflow-path* (on UNIX platforms)

For workflows running in the Java-based Server, you can run the tool with one of the commands:

- **runJavaWf.bat** *workflow-path* (on Windows)
- **runJavaWf.sh** *workflow-path* (on UNIX platforms)

Or you can include the Java class into your Java application.

The one and only parameter of the batch file is the *workflow-path*. This is a slash (/) separated list of display names as shown in the tree view of the DirX Identity Manager's Expert View.

Examples:

- `runwf.bat "Default/Source Scheduled/LDIFfile/LDIFFile2Ident"`

  Traverses the tree beginning with the node "workflows" and finds the corresponding workflow by comparing the display names. In this case, it starts the workflow **Meta2LDIFfile_Full** located in the sub-folder **Default/Source Scheduled/LDIFfile/LDIFFile2Ident**. As shown in the example above, a workflow path which contains blanks must be enclosed with double quotes, for example "my name".

- `java -cp … siemens.dxm.tools.RunWorkflow -cfg runwf.cfg`

  This is a direct call of the Java class without a batch file. It reads the configuration file **runwf.cfg** and starts the related workflow. **runwf.cfg** contains all relevant parameters and should appear as follows:

  ```
  tf=trace.out
  trace=3
  name=default/Source Scheduled/LDIFfile/LDIFfile2Ident
  ```

6.6.2.1. Parameters

The batch file contains a set of parameters. The option **-cfg** *filename* allows you to store all parameters to be loaded from a file. The valid parameters and their options are:

- **name** - a list of display names which qualify the workflow to be started. For example:

Default/Source Scheduled/LDIFfile/LDIFFile2Ident.

- **dn** - starts the workflow with this distinguished name. Note that either **-name** or **-dn** must be provided.
- **host** - the LDAP server's hostname. This is the server where the Connectivity configuration resides. The default value is **localhost**.
- **port** - the LDAP server's port. The default value is **389**.
- **rootDN** - the distinguished name (DN) of the configuration data's root. The default value is **dxmc=dirxmetahub**.
- **user** - the bind profile that will be used. The default value is **cn=server_admin,dxmc=dirxmetahub**.
- **password** - the bind profile's password. Specifying this parameter in the batch file or configuration file is deprecated for security reasons. Instead it should be absent. If absent, the password is taken from the property **ldap** of the file **password.properties** of the installation folder of this tool. It will be stored back in encrypted form for security reasons.
- **auth** - the authentication type. Anonymous and simple (the default) are currently supported.
- **initiator** - setting this switch allows you to distinguish between several **runwf** instances. This value is transferred to the **Initiator** field in the corresponding workflow status entry. The default value is **extern**. This parameter is only used for workflows running in the C++-based Server.
- **tf** (or equivalently: **tfile**) - the trace file where the trace output will be written. If absent, no trace output will be written. The placeholder **<?Localtime/>** (case-sensitive) expands to a timestamp representing the current time. When using this placeholder in a productive environment, it is your responsibility to clean up the resulting trace files.
- **timeoutCreate** - after sending the workflow create message, the **runwf** tool waits this number of seconds for a reply (this is normally fractions of a second). This switch prevents deadlocks at this point. A value of **0** or absence of this parameter or command-line option, respectively, denotes infinite waiting. This parameter is only used for workflows running in the C++-based Server.
- **timeoutExecute** - after sending the workflow execute message, the **runwf** tool waits this number of seconds for a reply. This switch prevents deadlocks at this point. A value of **0** or absence of this parameter or command-line option, respectively, denotes infinite waiting. This parameter is only used for workflows running in the C++-based Server.
- **statustracker** - delivers status tracker messages to the log file (can be used for debugging)
  off - Status tracker messages are not written to the log file (default)
  on - Status tracker messages are written to the log file
  This parameter is only used for workflows running in the C++-based Server.
- **trace** - trace level. The following levels are supported:
  0 - none
  1 - default
  2 - detailed
  3 - verbose

6.6.2.2. Exit Codes

The batch file (and the Java class) will return **0** to indicate successful execution.Otherwise, the return code has the following meaning:

- **1** - internal error (critical)
- **2** - destroy instance failed.Can't destroy the previously created workflow instance.This return code is only relevant for workflows running in the C++-based Server.
- **3** - unbind from the C++-based Server failed.This return code is only relevant for workflows running in the C++-based Server.
- >3 - an error number delivered by either the message service or the C++-based Server.This return code is only relevant for workflows running in the C++-based Server.

6.7. Using the Run Report Tool

The run report tool allows you to start reports from any location inside the network from the shell level.The tool is Java-based and can run on all DirX Identity supported platforms.The tool does not need any other parts of the DirX Identity system installed.You can use it to start reports triggered by any event outside DirX Identity.

The functionality to execute a report is provided as a Java class (siemens.dxm.report.Main), the delivered batch files act as wrappers.The tool connects to the configuration database (via LDAP) and then reads the bind credentials to establish a connection to the DirX messaging service.If this action succeeds, subsequent messages are sent to the appropriate C++-based Server to start and monitor the report.

6.7.1. Installing the Run Report Tool

To install the run report tool:

- The Java Runtime Environment (JRE) must be installed on the machine.(See the readme file on the DVD for the version supported.)
- A zip or tar file is delivered with DirX Identity in the folder: *install_path***tools\utilities\runReport.zip** (on Windows) or *install_path***tools\utilities\runReport.tar** (on UNIX)
- Extract the file **runReport.zip** to any file directory of your choice on Windows platforms.
- Unpack the file **runReport.tar.gz** (using gunzip and tar) into any file system directory on Linux platforms. Perform **chmod 755 runReport.sh**.

6.7.2. Running the Run Report Tool

You can run the tool with one of the commands:

- **runReport.bat** *report-name report-type* (on Windows)
- **runReport.sh** *report-name report-type* (on Linux)

Or you can include the Java class into your Java application.

Example:

- **`runReport.bat Default/Generic HTML`**

  Runs the Generic report in HTML format.

- **`java -cp … siemens.dxm.report.Main -cfg runReport.cfg`**

  This is a direct call of the Java class without a batch file. It reads the configuration file **runReport.cfg** and executes the related report. **runReport.cfg** contains all relevant parameters and should appear as follows:

```
tf=trace.out
tr=3
password=dirx
name=default/LDIFFile/Meta2LDIFfile_Full
```

6.7.2.1. Parameters

The batch file contains a set of parameters. The option **-cfg** *filename* allows you to store all parameters to be loaded from a file. The valid parameters and their options are:

- **name** - a list of display names which qualify the report to be executed. For example: default/Generic
  If the path contains blanks, you should enclose it with double quotes, for example "my name". Start qualifying the report name from the node "dxmC=reports,dxmC=GUI,dxmC=Configuration,dxmC=DirXmetahub". Note that either **name, dn** or **f** must be provided.
- **dn** - executes the report with this distinguished name. Note that either **name**, **dn** or **f** must be provided.
- **f** - define a file path that contains the report definition. Note that either **name**, **dn** or **f** must be provided.
- **type** - the report type, for example HTML or XML.
- **host** - the LDAP server's host name. This is the server where the Connectivity configuration resides. The default value is **localhost**.
- **port** - the LDAP server's port. The default value is **389**.
- **ssl** - indicates whether SSL shall be used for authentication. Allowed values are **true** and **false**.
- **user** - the bindprofile that will be used. The default value is **cn=server_admin,dxmc=dirxmetahub**.
- **password** - the bind profile's password.
- **auth** - the authentication type. Anonymous and simple (the default) are currently supported.
- **rootDN** - the distinguished name (DN) of the configuration data's root. The default value

is **dxmc=dirxmetahub**.

- **base** - the node at which to start object processing for this report. For example: **dxmC=Default,dxmC=Status Data,dxmC=DirXmetahub**.
- **scope** - the scope for searching the objects to process. The default is **subtree**. Allowed values are
  base object - the base object itself
  one level - use only objects of the next level under the base object
  subtree - use all objects beneath the base object
- **o** - the output path to which the report result is to be written.
- **trace** - trace level. The following levels are supported:
  0 - none
  1 - default
  2 - detailed
  3 - verbose

6.7.2.2. Exit Codes

The batch file (and the Java class) will return 0 to indicate successful execution. Otherwise, the return code has the following meaning:

- **1** - internal error (critical)

Appendix A: Deprecated Features

This chapter describes features in DirX Identity that are obsolete and will not be supported in future DirX Identity releases.

A.1. Deprecated Export Features

The following export features from previous DirX Identity versions are obsolete because the collection and transport mechanism is more powerful and fully customizable.These features will be removed in one of the next versions.

The described import features are still valid.

A.1.1. Exporting Parts of the Configuration Database

You can export parts of the configuration database.These options exist:

- **Logical object tree** - The logical DirX Identity object structure with all its links is evaluated and all detected objects are written to an LDIF file.You can write the file to any location, and you can import these files into the same or another configuration database.Use the **Export Data** function in the expert view to perform this operation.This function is useful when exporting a set of objects only a few times.
- **Structural object tree** - Allows to export an object and all of its sub objects in the LDAP tree. No links are followed in this case. Use the **Export Subtree** function in the Expert View to perform this operation. This function is useful when exporting a set of object only a few times.

Exports can be done on any object which then acts as a starting point for the data extraction. Possible objects are scenarios, workflows and jobs including all of their sub-objects defined by links or in the LDAP tree structure. For more information about the Export context menu selections, see the section "Using the Context Menu".

You can use these features for **backups** or **snapshots**, which help to reset to a specific state of your configuration database. You can also use them to **exchange logical or structural object trees,** for example from a test environment to a productive environment. In the case of logical object trees a **ToDo** file is written which helps to identify parts of the object tree which may not fit. Possible objects in this category are C++-based Servers, services and messaging objects.

To perform an export/import sequence:

1. Select the object you'd like to export in the expert view. Select **Export Data** or Export Subtree from the context menu. Alternatively you can create an object collection and export the related objects based on this collection.
2. A file selection box opens which allows you to define the file name and the location of the file.
3. To import such an LDIF file, select the root node of the Connectivity configuration tree and select **Import Data** from the context menu.

Do not import data from previous or later versions of DirX Identity. Important attributes could be missing or are contained which will results in an error during the import operation or in strange behavior of the DirX Identity Manager after the import operation. Instead, import such workflows into your database, perform the upgrade installation including a migration.

4. The file dialog opens again, and you can select the required file. Click **Open** to start the import procedure.

Be aware that an import of this information from the LDIF file only overwrites existing objects and attributes. New attributes or objects you created between the export and the import are not touched. Thus you perform a merge.

Import Data Features

In addition to former versions, now referenced Agent object are also exported during an **Export Data** procedure and therefore are transferred via **Import Data** to your target system. This is especially useful if you have created your own agents.

Additionally, you can define a mapping of dxmService-DN / dxmMetahubSyncServer-DN references. Assume we have a test and a production environment. Each environment has specific Services and MetahubSyncServer entries (because they run on different machines). You have developed a new workflow in your test environment, and you export it via **Export Data** to an LDIF file. Now you import it via **Import Data** to your production environment. As all dxmService-DN / dxmMetahubSyncServer-DN's reference objects of the test environment, you have to correct all these references by hand to the appropriate objects.

To avoid this task during every import two mechanism are available. DirX Identity tries to find an object with the same display name. This works in all cases where a display name is available. Alternatively you can define a DN-mapping.

Use the file **referenceDNmapping.tcl** in *install_path*/Tools/Import. Here you can define an Tcl array indexed by the dn that contains the displayname of the corresponding object. The file contains already some sample entries. It is assumed, that the object with the given dn has the given displayname and that the object with this displayname in the target (production) environment is identical with the object in the source (test) environment.

For more information about the Import context menu selections, see the section "Using the Context Menu".

Integrating Workflows into a Scenario

Please note that workflows which are imported from one configuration database to another one do not automatically appear in a scenario. There are two ways to solve this issue:

- Export and import the complete scenario. This includes all workflows contained in that scenario.
- Insert the workflow into one of your scenarios. You can perform this step:

- in the scenario object in the Expert View by adding workflows to a workflow line (be sure to take the right one)
- with the function **Assign** from the context menu of a workflow line in the Global View.

A.1.2. Exporting the Entire Configuration Database

You can export the entire configuration database tree to a flat LDIF file (**Export Configuration**), and then re-import it with **Import Data** or **Replace Configuration**. All objects of the configuration database are exported.

You can use this function for **backups** or **snapshots**, which help to reset to a specific state of your configuration database.

Please be aware that an import of this information from the LDIF file with **Import Data** does only overwrite existing objects and attributes. New attributes or objects you created between the export and the import are not touched. Thus, you perform a merge. To replace the whole configuration tree you need to use **Replace Configuration**.

Do not import data from previous versions of DirX Identity. Important attributes could be missing which will results in strange behavior of the DirX Identity Manager.

DirX Product Suite

The DirX product suite provides the basis for fully integrated identity and access management; it includes the following products, which can be ordered separately.

DirX Identity

DirX Identity provides a comprehensive, process-driven, customizable, cloud-enabled, scalable, and highly available identity management solution for businesses and organizations. It provides overarching, risk-based identity and access governance functionality seamlessly integrated with automated provisioning. Functionality includes lifecycle management for users and roles, cross-platform and rule-based real-time provisioning, web-based self-service functions for users, delegated administration, request workflows, access certification, password management, metadirectory as well as auditing and reporting functionality.

DirX Directory

DirX Directory provides a standards-compliant, high-performance, highly available, highly reliable, highly scalable, and secure LDAP and X.500 Directory Server and LDAP Proxy with very high linear scalability. DirX Directory can serve as an identity store for employees, customers, partners, subscribers, and other IoT entities. It can also serve as a provisioning, access management and metadirectory repository, to provide a single point of access to the information within disparate and heterogeneous directories available in an enterprise network or cloud environment for user management and provisioning.

DirX Access

DirX Access is a comprehensive, cloud-ready, scalable, and highly available access management solution providing policy- and risk-based authentication, authorization based on XACML and federation for Web applications and services. DirX Access delivers single sign-on, versatile authentication including FIDO, identity federation based on SAML, OAuth and OpenID Connect, just-in-time provisioning, entitlement management and policy enforcement for applications and services in the cloud or on-premises.

DirX Audit

DirX Audit provides auditors, security compliance officers and audit administrators with analytical insight and transparency for identity and access. Based on historical identity data and recorded events from the identity and access management processes, DirX Audit allows answering the “what, when, where, who and why” questions of user access and entitlements. DirX Audit features historical views and reports on identity data, a graphical dashboard with drill-down into individual events, an analysis view for filtering, evaluating, correlating, and reviewing of identity-related events and job management for report generation.

For more information: support.dirx.solutions/about

Legal remarks

On the account of certain regional limitations of sales rights and service availability, we cannot guarantee that all products included in this document are available through the Eviden sales organization worldwide. Availability and packaging may vary by country and is subject to change without prior notice. Some/All of the features and products described herein may not be available locally. The information in this document contains general technical descriptions of specifications and options as well as standard and optional features which do not always have to be present in individual cases. Eviden reserves the right to modify the design, packaging, specifications and options described herein without prior notice. Please contact your local Eviden sales representative for the most current information. Note: Any technical data contained in this document may vary within defined tolerances. Original images always lose a certain amount of detail when reproduced.