i-net Clear Reports 2017

Security Guide

Configuration of Permissions

i-net software

© Copyright 1996 - 2017, i-net software GmbH; All rights Reserved.

1 Content

Security is an important feature for reporting software. There are many conceivable cases where it would be necessary to restrict the rights on the reports. You may not want all users to be able to execute just any report and to thereby gain access to almost all data in your database. This can be configured using the report permissions in the report repository.

It might also be necessary to limit the locations from which it is possible to take reports and execute them. This will prevent someone from executing unknown reports on the report server. This can be configured using Report Locations.

With Permissions it is possible to control the access to the remote features and to allow access to all reports.

© Copyright 1996 - 2017, i-net software GmbH; All rights Reserved.

2 Concepts of the Report Permissions

i-net Clear Reports does not have its own login database. It instead uses the login information on the current system or external servers.

2.1 Security Mechanisms

There are the following 2 security mechanisms available.

2.1.1 Report Locations

With report locations you can limit the locations from which reports can be loaded for execution. Only reports from the given locations and their sub-folders will be permitted to be executed. This does not require any user information. The default option is that it is possible to open reports from all local (server) and file locations.

2.1.2 Report Permissions

With report permissions it is possible to set access rights for specific users or user roles in the repository browser. This requires the login information of the current user. There are several ways to receive this login information:

- login on the current web server with Windows, PAM or Application Server credentials
- a login script authenticating using another server
- login on by using a database or LDAP

The concepts are described below.

2.2 System Requirements

If you want to protect your reports or parts of the reports from anonymous access, you'll have to set a valid login configuration for i-

© Copyright 1996 - 2017, i-net software GmbH; All rights Reserved.

net Clear Reports. Installing i-net Clear Reports can be done on any server with at least Java 7 installed. Integration with Application Server or Web servers is possible but not necessary. Depending on the selected authentication method an external authentication provider may be required.

© Copyright 1996 - 2017, i-net software GmbH; All rights Reserved.

3 Authentication

In order to use the security features of i-net Clear Reports, you'll have to set up an authentication method. The method to be used can be set while installing the product and in the configuration manager on the 'Login' panel.

i-net Clear Reports provides a large set of authentication methods. Please note that some of them depend on the installed operating system and/or the server application in use.

3.1 Authentication methods

i-net Clear Reports provides the following authentication methods (login types) by default:

- **Automatic:** This default value allows i-net Clear Reports to determine the available method automatically. The server tries to request the login in the following order: External web server (a Login URL must be set), LDAP Authentication (if the Login URL starts with ldap or ldaps), Windows Authentication (if the server is running on a Windows operating system), PAM Authentication (if the server is running on a non Windows server and if it was possible to load the PAM library), Internal web server, Master Password.
- **External web server:** With this setting, a Login URL to an external web server can be defined. Users will then have to authenticate against this web server. If no (or no valid) Login URL has been defined, a fallback to Master Password authentication is performed.
- **LDAP Authentication:** With this login type a LDAP server will be used for authentication. If the URL is empty, the LDAP server will searched in the DNS of the current domain. Sample login URL: `ldap://MyLdapServer:389/` or `ldaps://MyLdapServer:636/` (with SSL).
- **Windows Authentication:** If the server runs on a **Windows operating system**, users will automatically be logged into the system with their Windows accounts. If the server's operating system is not Windows, a fallback to Master Password authentication is performed.
- **PAM Authentication:** This login type can be used if i-net Clear Reports

© Copyright 1996 - 2017, i-net software GmbH; All rights Reserved.

runs on **Linux or Mac OS X**. It can be configured using the file "/etc/pam.d/reporting". If it does not exists, then "/etc/pam.d/passwd" will be used as fallback.

- **Database Server:** With this login type a database server will be used for authentication. As a prerequisite, the jar file of the database driver needs to be in the lib directory of the report server (a server restart is necessary after the jar file was added). As Login URL you need to set a valid JDBC URL (see documentation of the used JDBC driver). With MS SQL server and the driver i-net Merlia (included with i-net Clear Reports), NTLM can be used.
  This database login can also be used for reports, e.g. to filter the data for the logged in user. To do this you need to create a datasource configuration with the database class com.inet.report.authentication.database.LoginDatabase and use it in the report.
- **Internal web server:** If i-net Clear Reports is installed and running in an **application server** such as Apache Tomcat, the authentication system provided by the application server is used. For example: the default user administration of Apache Tomcat takes place in the file: tomcat-users.xml. If there is no authentication system active in the application server, a fallback to Master Password authentication is performed.
- **Master Password:** If no login URL or application server with active authentication system is available, the user can log into the Remote-Interface using a password that is defined by the administrator. The password should have been defined during setup or has to be set with the first access to the Remote-Interface. Using Master Password authentication, users will only have access to restricted modules, when they log into the Remote Interface, however not to any restricted reports. A direct authentication for reports or interfaces is not possible.

3.1.1 Login URL

If the authentication method is set to "Automatic" or "External Webserver", a URL to a Login Script may be defined. You can use the default LoginServlet (single server only) by not setting a URL or an external login script. To verify the correctness of the login URL, please enter this URL in a normal web browser:

© Copyright 1996 - 2017, i-net software GmbH; All rights Reserved.

```
http://localhost/clearreports/LoginServlet

# or

http://localhost/YourPath/login.aspx
```

Now your browser should request for login information. How this request is presented depends on how you have configured the login of your web application server (BASIC, FORM, etc.). With a successful login in the browser you will receive an XML file like:

```
<properties>
 <entry key="username">scott</entry>
</properties>
```

If you see an error page, your configuration is incorrect. In that case and if you're using the LoginServlet, a change in web.xml, which is located in the reporting.war, can be necessary depending on the used application server. See the documentation of your application server or servlet engine for more details.

Note: If the login script administrates the user by domain **and** user name (as in "DOMAIN/User"), the permissions have to be configured the same way later on.

3.1.2 Internal web server

This authentication method is only available if i-net Clear Reports is installed in an application server or servlet engine. The configuration of the users and roles for that method depends on the application server.

Important: Please refer to the documentation of the application

© Copyright 1996 - 2017, i-net software GmbH; All rights Reserved.

server for setting up the credentials.

Some application server allow to define different credential stores for each application or to use a single store. This is important if you're planning to use Single Sign On.

Once you've defined the users and roles in the realm of your application server, you have to modify the web.xml of i-net Clear Reports to use the roles in the application as well. The location of this file depends on the application server. Add the roles to be used to the XML file:

```
   ...
   <security-role>
      <role-name>users</role-name>
   </security-role>
   <security-role>
      <role-name>guests</role-name>
   </security-role>
</web-app>
```

3.1.3 Custom Authentication

As of Version 14 i-net Clear Reports allows to extend the authentication methods by adding plugins to the application. To create a custom authentication mechanism, you'll have to create a plugin as described in the "Server Programming Guide".

The Plugin has to implement the following Interfaces:

- `com.inet.authentication.AuthenticationProvider`
- `com.inet.authentication.WebUserInfo`
- `com.inet.authentication.UsersAndGroupsProvider`
- `com.inet.plugin.ServerPlugin`

© Copyright 1996 - 2017, i-net software GmbH; All rights Reserved.

These interfaces are located in the `inetcore.jar` in the 'core' folder of i-net Clear Reports. Their API documentation can be found either in the installed documentation or online.

To enable i-net Clear Reports to load and use your AuthenticationProvider, your implementation of the `ServerPlugin` interface requires at least:

```
@Override
public void registerExtension( ServerPluginManager spm ) {
    spm.register( AuthenticationProvider.class, new
MyCustomAuthenticationProvider() );
}
```

The methods init, reset and restart can be left empty.

3.2 Single Sign On

When using a website or web application combined with i-net Clear Reports it's recommended to only let the user log-in once. The solution for this scenario depends on your server infrastructure and selected authentication method.

3.2.1 Single Server

In this configuration, i-net Clear Reports would be running in an application server that presents your web front-end or web application as well. It's recommended to set the authentication method to '**Internal web server**' for that use case. This enables i-net Clear Reports to share the session and authentication with your web application.

Pro	Contra

© Copyright 1996 - 2017, i-net software GmbH; All rights Reserved.

Pro	Contra
Easy and seamless integration with web applications	Requries an application server

If you require another authentication method or i-net Clear Reports runs in a separate process (e.g. IIS or Apache with PHP), make sure that i-net Clear Reports is accessed by the same host name as your front-end server. Furthermore, the credential store has to be the same for the web application and i-net Clear Reports. This is required to enable the client browser to automatically resend the authentication when switching between the web application and i-net Clear Reports. The user won't be notified about this re-login so the user experience is seamless.

Pro	Contra
Works with almost any web server	Requires basic or NTLM authentication
	Both server applications must have the same credentials base

3.2.2 Front-end + Back-end Server

In case you want to install i-net Clear Reports on a firewall-protected back-end server, a different setup for authentication has to be used. Since your web site or application is hosted on another (front-end) server, i-net Clear Reports has to contact this server to share the authentication. Make sure, this connection is not blocked by the firewall as well.

To set up this solution please:

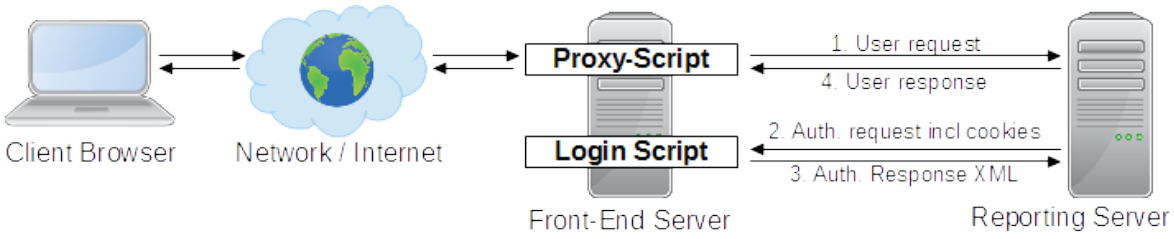
- Setup a Proxy on the front end server. This can be done by using the PHP or the ASPX proxy script located in the samples folder of the i-net Clear

© Copyright 1996 - 2017, i-net software GmbH; All rights Reserved.

Reports installation. If you're using another proxy, make sure to forward all cookies and/or the authentication header to the i-net Clear Reports server.

- Install a login script on the front-end server. See Login Script section for details.
- Make sure the back-end server can contact the front-end server for the Login Script
- Configure i-net Clear Reports to the authentication method 'External web server' and set the 'Login URL' to the location of the Login Script on the front-end server

How it works in production:



It's important in this scenario, that request 1. and 2. pass all cookies (session ID) and header (authentication header). This allows the Login Script on the front-end server to identify a user by session cookie or by authentication.

Pro	Contra
Allows Firewall protection for the back-end server	Additional load on the front-end server
Single entry point (host) for users	May require a custom proxy implementation

3.2.3 Parallel Servers

In this scenario the web site/application server and the server hosting i-net Clear Reports are both connected to the same network or the internet. The user can directly access both servers. So in

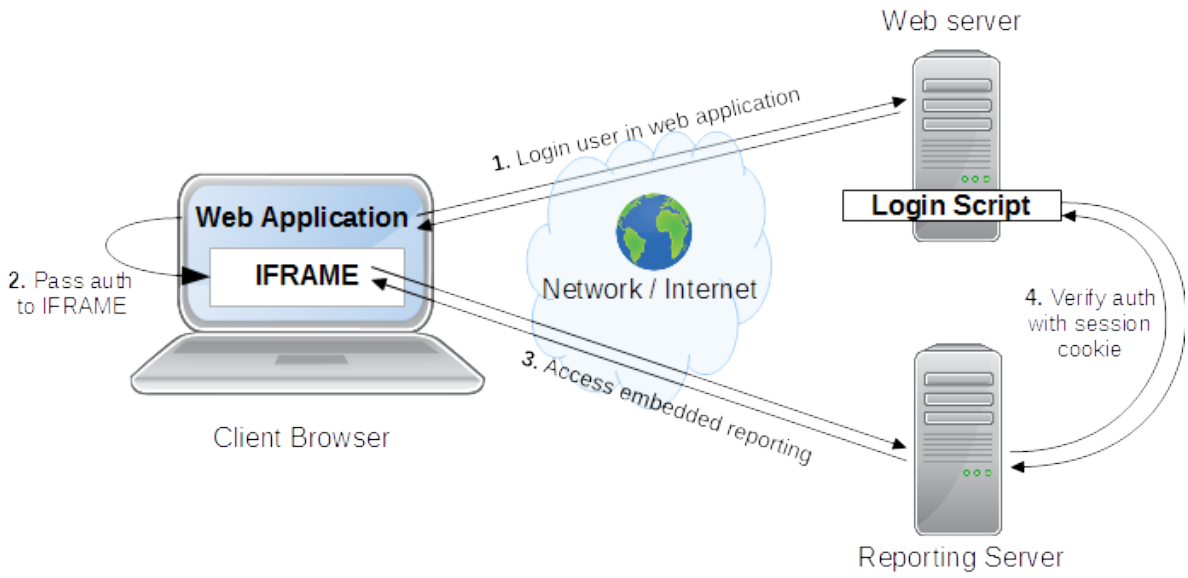
© Copyright 1996 - 2017, i-net software GmbH; All rights Reserved.

contrast to the front-end / back-end architecture, there is no proxy which can pass the authentication or session data from the web site/application server to the reporting server. So passing the session cookie has to be done by the web site running in the browser of the client/user. For that reason, a front-end / back-end solution is recommended in most cases.

To set up this solution please:

- Install a login script on the web site/application server, see Login Script section for details.
- Modify your web site or application to present the i-net Clear Reports report or web interface in an IFRAME embedded in your web site/application
- Modify your web web site or application to pass the session cookie to this IFRAME so that the IFRAME uses this cookie when querying the reporting server
- Configure i-net Clear Reports to use the authentication method 'External web server' and set the 'login URL' to the location of the login script on the web site/application server.

How it works in production:



© Copyright 1996 - 2017, i-net software GmbH; All rights Reserved.

As you can see, the most critical point here is to pass the session from your web application to the reporting IFRAME. Most browsers will try to prevent you from re-using a cookie for another host. So it requires sophisticated JavaScript knowledge to implement such solution.

Alternatively you may pass the required session data as URL parameters to the IFRAME. But since i-net Clear Reports only passes Cookies and HTTP header fields to the Login Script, this would require to extend the reporting server with a plugin to convert the URL parameters to a cookie for authentication.

Pro	Contra
No proxy required	Requires sophisticated JavaScript or Java coding
No extra load for the web server	Exposes back-end architecture

3.3 Login Script

The authentication method 'External web server' requires the requested location to perform the authentication and to return a valid response in XML format.

To enable the external web server to authenticate the user, i-net Clear Reports sends all cookies (e.g. the session cookie) and the HTTP authentication header of the original request along with it's request to the authentication server.

In case the authentication server is able to authenticate the user, it has to respond with XML content that contains the user's username, e.g. sending a valid authentication for user "JohnDoe", the

© Copyright 1996 - 2017, i-net software GmbH; All rights Reserved.

authentication server should respond:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<entry key="username">JohnDoe</entry>
</properties>
```

Important: You have to make sure that the user name is always returned in way that is unique to the system (e.g. always make it lowercase - even if the user logs in with uppercase letters) - the reason behind this is: i-net Clear Reports supports case-insensitivity in every permission checking context, but it will respect folder names case-sensitively. If you had a user named "JohnDoe" and he logs into the system with "johndoe" there would be two different home directories in the repository though you meant the same user.

To check whether a user is in certain roles, i-net Clear Reports will attach the roles to check as parameters to the request URL. The server than has to check for each role and extend the XML appropriately:

```
REQUEST:
http://<YourServer>/login.aspx?abc=&somerole=

RESPONSE:
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<entry key="username">JohnDoe</entry>
<entry key="abc">False</entry>
<entry key="somerole">True</entry>
</properties>
```


© Copyright 1996 - 2017, i-net software GmbH; All rights Reserved.

Using roles is a convenient way to specify restrictions for many users at once. Furthermore you can even use the roles in the formulas of a report to adapt the report to the executing user. The formula function to check a role is isWebUserInRole(<roleName>).

For the most common cases of authentication servers running ASP.NET, PHP or Java Server Pages, please use the following samples as a reference:

3.3.1 ASP.NET Sample

Create a file with the extension *.aspx (e.g. login.aspx) in the IIS and copy the following script into this file. Enable the authentication method "Basic authentication" for this .aspx file in the IIS configuration.

An installed Microsoft .Net Framework version 2.0 or higher is required to execute this script.

```
<%@ Page Language=VB ResponseEncoding="utf-8" %>
<%
If User.Identity.Name = "" Then
 Response.Write( "401 Access Denied" )
 Response.Status = "401 Access Denied"
 Response.End
end if
Response.ContentType = "text/xml; charset=utf-8"

Response.Write( "<?xml version=""1.0"" encoding=""UTF-8""?>" & Chr(10))
Response.Write( "<!DOCTYPE properties SYSTEM
""http://java.sun.com/dtd/properties.dtd"">" & Chr(10))
Response.Write( "<properties>" & Chr(10))

Response.Write( "<entry key=""username"">" &
Server.HTMLEncode(User.Identity.Name) & "</entry>" & Chr(10) )
```


© Copyright 1996 - 2017, i-net software GmbH; All rights Reserved.

```
Dim Key
For Each Key In Request.QueryString
    if Key <> "" Then
        Try
            Response.Write("<entry key=""" & Server.HtmlEncode(Key) &
""">" & Server.HtmlEncode(User.IsInRole(Key)) & "</entry>" & Chr(10))
        Catch
            Response.Write("<entry key=""" & Server.HtmlEncode(Key) &
""">false</entry>" & Chr(10))
        End Try
    End If
Next

For Each Key In Request.Form
    if Key <> "" Then
        Try
            Response.Write("<entry key=""" & Server.HtmlEncode(Key) &
""">" & Server.HtmlEncode(User.IsInRole(Key)) & "</entry>" & Chr(10))
        Catch
            Response.Write("<entry key=""" & Server.HtmlEncode(Key) &
""">false</entry>" & Chr(10))
        End Try
    End If
Next
Response.Write( "</properties>" & Chr(10))
%>
```

3.3.2 JSP Sample

Create a file with the extension *.jsp and copy it into any web context.

```
<%@page language="java" contentType="text/xml; charset=utf-8"
pageEncoding="UTF-8"
import="java.security.Principal"
import="java.io.*"
import="java.util.*"
```


© Copyright 1996 - 2017, i-net software GmbH; All rights Reserved.

```
%><%!
public static String encode(String s){
 StringBuilder out = new StringBuilder();
 for(int i=; i<s.length(); i++){
  char c = s.charAt(i);
  if(c > 127 || c=='"' || c=='<' || c=='>'){
   out.append("&#"+(int)c+";");
  }else{
   out.append(c);
  }
 }
    return out.toString();
}

%><?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<%
 Principal p = request.getUserPrincipal();
 if( p != null ){
  out.write( "<entry key=\"username\">" + encode( p.getName() ) +
"</entry>\n" );
 }

 Enumeration e = request.getParameterNames();
 while(e.hasMoreElements()){
  String key = (String)e.nextElement();
  key = new String( key.getBytes("ISO8859_1"), "UTF8");
  out.write( "<entry key=\"" + encode( key ) + "\">" +
request.isUserInRole(key) + "</entry>\n" );
 }
%>
</properties>
```

3.3.3 PHP Sample

Create the files .htaccess, .htpasswd and .htgroups. This file can look

© Copyright 1996 - 2017, i-net software GmbH; All rights Reserved.

like this:

.htaccess

```
# dont allow htaccess and htpasswd
<Files ~ "^.(htaccess|htpasswd)$">
deny from all
</Files>

# .htpasswd contains the password and users
AuthUserFile /opt/lampp/htdocs/.htpasswd
AuthGroupFile /opt/lampp/htdocs/.htgroups
AuthName "Please enter your ID and password"
AuthType Basic
require valid-user
```

.htpasswd - A user test with password test.

```
test:WCt/yYmXR2kLA
```

.htgroups

```
admin: test
```

Create a php login file with the following content:

```
<?php
  // This is the .htgroups file - the web server requires to have read
permission for this file!
  $AuthGroupFile = file("/path/to/.htgroups");

  // If the Apache has AUTH Info, set them for PHP as well
  if (!empty($_SERVER['AUTH_USER']))
  {
```


© Copyright 1996 - 2017, i-net software GmbH; All rights Reserved.

```
    $_SERVER['PHP_AUTH_USER'] = $_SERVER['AUTH_USER'];
    $_SERVER['PHP_AUTH_PW']   = $_SERVER['AUTH_PASSWORD'];
  } else if (!empty($_SERVER['REMOTE_USER'])){
    $_SERVER['PHP_AUTH_USER'] = $_SERVER['REMOTE_USER'];
  }

  // Check whether someone has authenticated - if not, request another
Basic Authentication
  if (!isset($_SERVER['PHP_AUTH_USER'])) {
    header('WWW-Authenticate: Basic realm="Server Authentication"');
    header('HTTP/1.0 401 Unauthorized');
    echo 'Access Denied';
    exit;
  }

  // Here you may insert additional checks for the user, like querying a
database.
  // Alternatively this can be done via .htaccess in apache

  $return = '';
  $return .= '<entry key="username">' .
strtolower(htmlentities($_SERVER['PHP_AUTH_USER'])) . "</entry>\n";

  foreach ( $_REQUEST AS $key => $value ) {
    $status = !preg_grep("/$key:.*?\s" .
htmlentities($_SERVER['PHP_AUTH_USER'])  . "(\s.*?)?$/", $AuthGroupFile)
? 'false' : 'true';
    $return .= '<entry key="' . htmlentities($key) . '">' . $status .
"</entry>\n";
        }

  header('Content-Type: text/xml; charset=utf-8');
  print <<<OUTPUT
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
$return
</properties>
OUTPUT;
?>
```


© Copyright 1996 - 2017, i-net software GmbH; All rights Reserved.

© Copyright 1996 - 2017, i-net software GmbH; All rights Reserved.

4 Activation of the Security Features

Once you've configured an authentication method other than 'Master Password' you can configure the permissions in the configuration manager and the report permissions in the repository browser.

4.1 Activation of Report Locations

You can enable the check of the Report Locations in the i-net Clear Reports Configuration Manager.

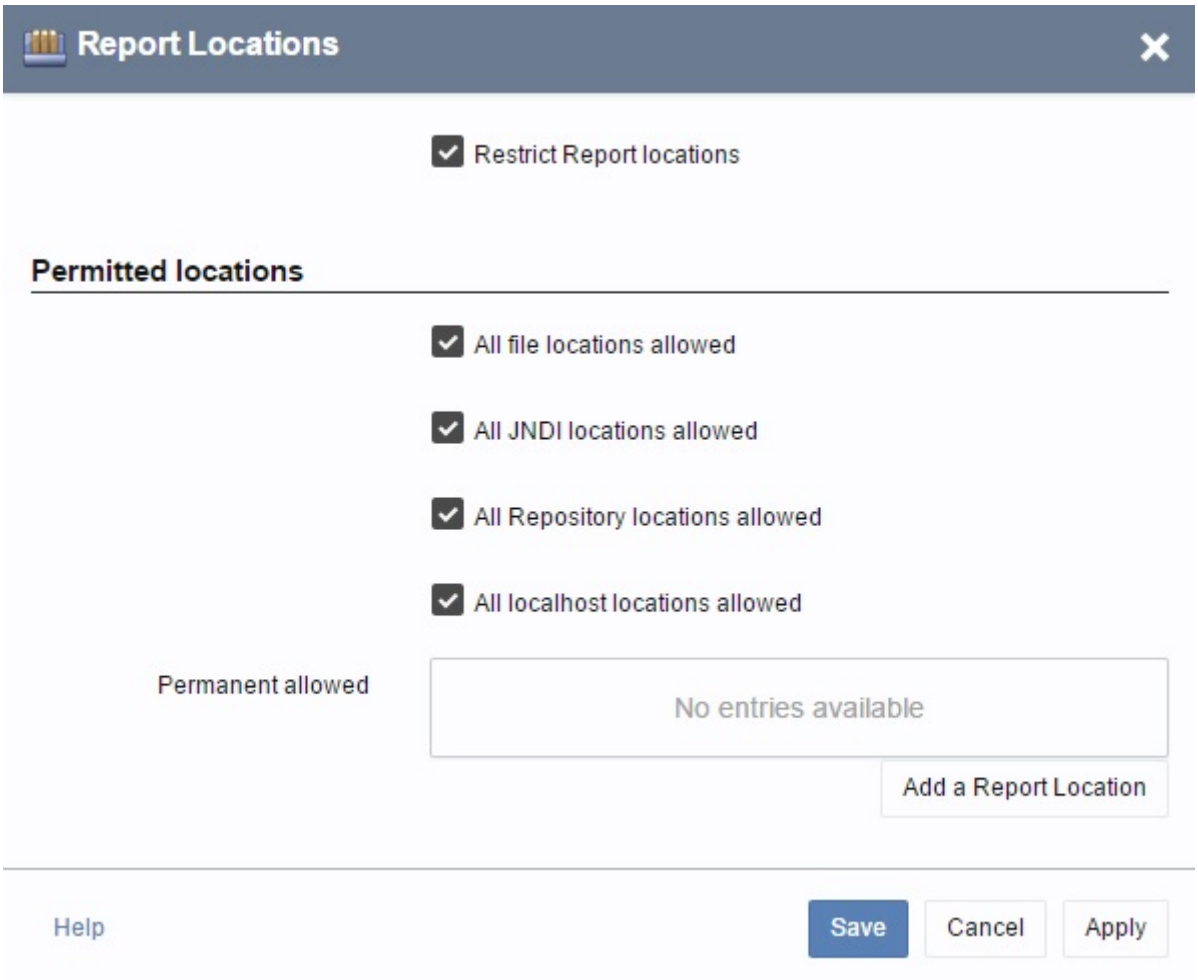


Figure 1: Configuration Manager – Report Locations

If you enable the check of the Report Locations then you should

© Copyright 1996 - 2017, i-net software GmbH; All rights Reserved.

enable "All file locations allowed", "All localhost locations allowed" or you must add at least one URL from that reports can be loaded by i-net Clear Reports.

4.2 Activation of the Permissions

You can enable the option "Restrict Permissions" in the i-net Clear Reports - Configuration Manager dialog "Permissions".

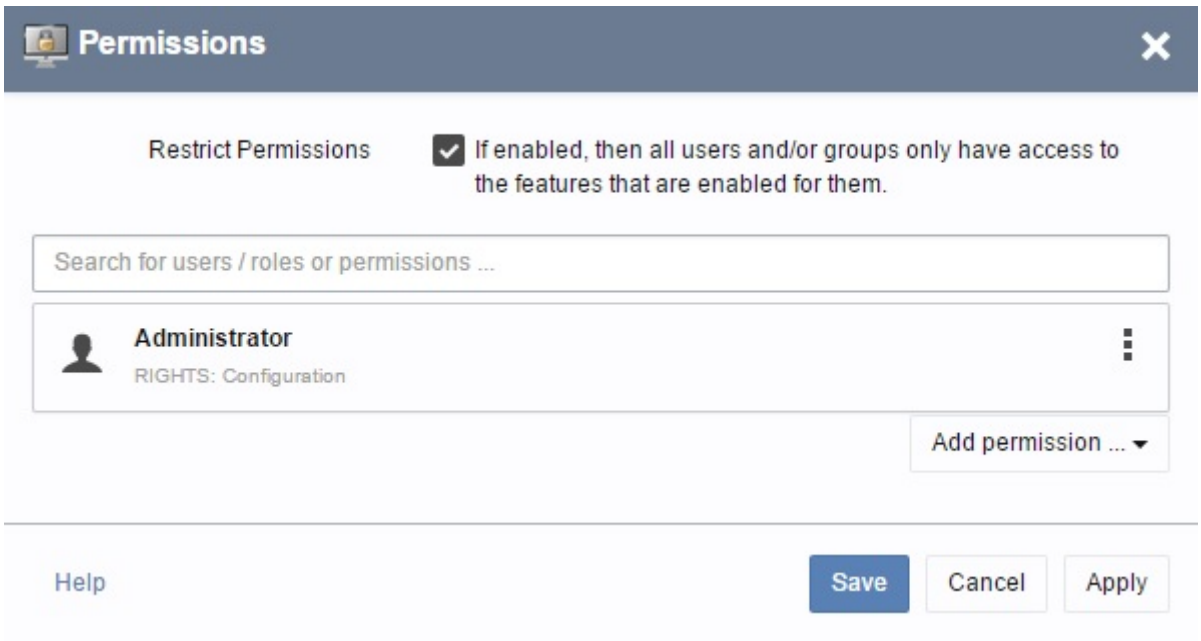


Figure 2: Configuration Manager – Permissions

If you enable "Restrict Permissions", you should configure at least one user or group for the feature "Configuration" so that it is possible for this user to execute the Configuration Manager in the Remote Interface. If you do not, no one will be able to access the Configuration Manager except by using the Configuration Recovery Tool which is located in the installation directory.

© Copyright 1996 - 2017, i-net software GmbH; All rights Reserved.

5 Features

5.1 Permissions

With permissions you can restrict the access to certain parts of the system and remote application such as ad hoc reporting. They permissions can be administrated using the Remote Configuration Manager.

The features are web applications in the i-net Clear Reports Remote Interface. Depending on the activated plugins the following permissions can be granted to a user / group:

- **Ad Hoc Data Sources:** allows the user or group to retrieve the remote data source of the server via the Remote Designer or the ad hoc reporting feature.
- **Ad Hoc Reporting:** allows the user or group to access the ad hoc reporting.
- **Configuration:** allows the user or group to access the remote Configuration Manager. This also allows granting permissions in the Repository Browser (with write-permission) and shows the folder 'All Users' of the User Directories if active.
- **Data Source Configuration:** allows the user or group to access the remote Data Source Configuration Manager.
- **Execute All Reports:** allows the user or group to execute all reports. If the user should execute only reports from the report repository then configure the permissions in the repository browser instead of using this permission.
- **Remote Designer:** allows the user or group to access the WebDAV interface (Context /repository) and the usage of the Remote Designer.
- **Remote Printing:** allows the user or group to print remotely on the server.
- **Repository:** allows the user or group to access the remote Repository Browser.
- **Task Planner:** allows the user or group to access the Task Planner.
- **Statistics:** displays statistical information about the server state, rendered and cached report etc.
- **XML-RPC:** allows the user to make use of the XML-RPC interface. For an

© Copyright 1996 - 2017, i-net software GmbH; All rights Reserved.

overview over which XML-RPC methods are offered, refer to the XML-RPC API page (Context /xmlrpc).

If the configuration has no valid authentication method set, you can log in to the Remote Interface as the system administrator using the master password. This user has no restrictions, each feature will be visible and can be used.

5.2 Report Locations

By default, any report in any location (local file system, external web server etc.) can be executed on your i-net Clear Reports server. That can make things easy for your employees and customers, but it can be a security issue as well.

To solve this problem and reduce security risks, you can grant access for certain report locations only. The report locations consist of a list of folders and URL's which contains report files that can be executed.

5.3 Repository Permissions

The Report Repository is a feature of i-net Clear Reports Plus which allows streamlined and simple central storage and execution of reports on the report server.

In addition to the permission "Execute All Reports" in the Configuration Manager, users with appropriate privileges can also manage report permissions directly from the Repository Browser. With the report permissions it is possible to restrict the access to reports in the repository depending on the currently logged in user.

The rights on a folder in the repository will be inherited by

© Copyright 1996 - 2017, i-net software GmbH; All rights Reserved.

subfolders. It is possible to list files in the repository when only an execution permission is granted. The read permission is not necessary anymore to list the report files.

A pattern can be used for report file names. It can contain characters, the asterisk symbol (*) as a wildcard for any number of symbols or the question mark (?) as a wildcard for a single symbol. After a pattern has been created, you have to define at least one user name or group for the pattern. For users and groups you can use the asterisk symbol (*) as a wildcard as well. For instance if the group "admin" should have access to all reports, you have to create a new global pattern "*" for "all reports" and then give the group "admin" access to this pattern (which will match all reports).

The following permissions can be set:

- read
- write
- execute

For detailed information please have a look at the Repository Guide.

5.4 i-net Designer Properties

To test the security functions with i-net Designer, you can set the current web user name and its roles in the section "Virtual Permissions" of the "Designer Options..." (see menu "Options | Designer Options...") . Here you can enter the simulated user name and user roles.

5.4.1 Using restrictions within a report

The authentication credential can be used within reports using formula functions. The following 3 functions are available in the node

© Copyright 1996 - 2017, i-net software GmbH; All rights Reserved.

"Security Functions" of the Formula Editor:

- **WebUserName**
- **IsWebUserInRole(String)**
- **FireAccessDenied**

Using these functions in formulas, you can filter records in the Record Selection Formula, hide fields or sections, etc., depending on the WebUserName and/or the Role of the current user. With the FireAccessDenied function it is even possible to cancel the report execution if the current user is not logged on or is not a member of the specified roles (groups). It is possible to test these functions within the i-net Designer if "Restrict Permissions" is activated in the permission panel of the configuration used by i-net Designer and if a user name and/or roles have been specified in the "Designer Options" dialog.

© Copyright 1996 - 2017, i-net software GmbH; All rights Reserved.

6 Example Scenarios

6.1 Filtering with a Record Selection Formula

In case you have sensitive data in your database for different users and you want any user to only be able too see his or her own data then you can filter the data. A typical example is a ticket or billing system.

If you have a table column with the user names you could for instance set the Record Selection Formula to:

```
if WebUserName() = "" then
 fireAccessDenied()
else
 {YourTable.username} = WebUserName();
```

The call of the function fireAccessDenied is used to force a login for the user if they are not logged in yet.

© Copyright 1996 - 2017, i-net software GmbH; All rights Reserved.

7 Other Security Options

7.1 Restrictions

Note that i-net Clear Reports also has some other security options not related to a login. These are located in the section "Restrictions" of the dialog "Document Properties" in i-net Designer and include the following:

- Show Group Tree
- Allow Printing
- Allow Copy of Content
- Allow Export
- Allow the following output formats for the report

© Copyright 1996 - 2017, i-net software GmbH; All rights Reserved.

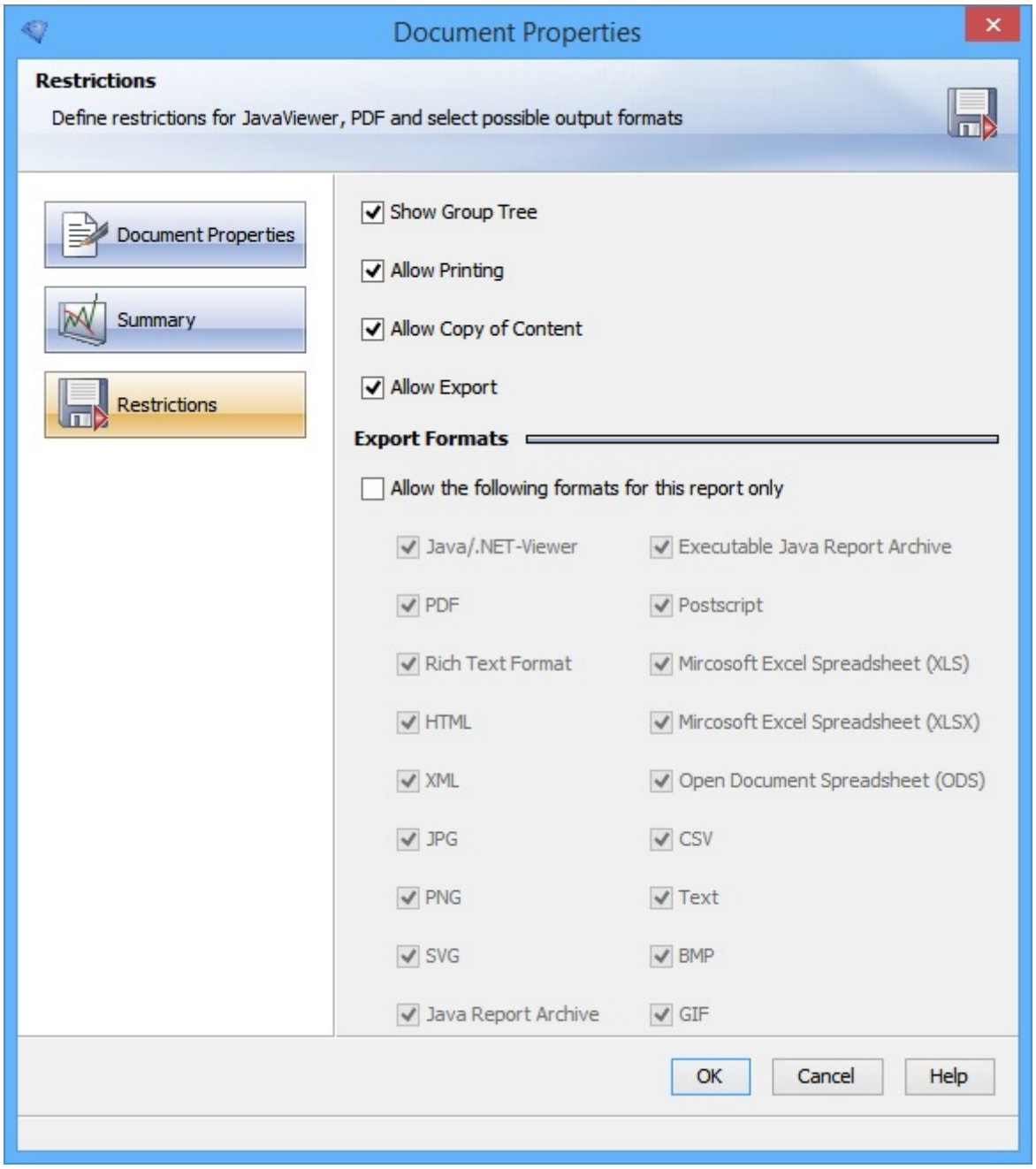


Figure 3: i-net Designer - Document Properties

7.2 Allow unknown Data Sources

For security reasons the property "Allow unknown Data Sources" can be disabled. You can find it in to the configuration dialog "Behavior".

If this property is disabled, it is not possible to execute reports

© Copyright 1996 - 2017, i-net software GmbH; All rights Reserved.

containing an unknown datasource. A data source is unknown if no data source configuration exists with this name on the report server. This will prevent the usage of report-defined databases and possibly insecure connections.

© Copyright 1996 - 2017, i-net software GmbH; All rights Reserved.