

RepliWeb

Proxy User Security Mechanism (Virtual Users)

For Windows, Linux and UNIX operating systems

May 17, 2011

Copyright © 2011 RepliWeb® Inc., All Rights Reserved

The information in this manual has been compiled with care, but RepliWeb, Inc. makes no warranties as to its accuracy or completeness. The software described herein may be changed or enhanced from time to time. This information does not constitute a commitment or representation by RepliWeb and is subject to change without notice. The software described in this document is furnished under license and may be used and/or copied only in accordance with the terms of this license and the End User License Agreement.

No part of this manual may be reproduced or transmitted, in any form, by any means (electronic, photocopying, recording or otherwise) without the express written consent of RepliWeb, Inc.

Windows, Windows NT and Windows XP are trademarks of Microsoft Corporation in the US and/or other countries. UNIX is a registered trademark of Bell Laboratories licensed to X/OPEN.

Any other product or company names referred to in this document may be the trademarks of their respective owners.

Please direct correspondence or inquiries to:

RepliWeb, Inc.
6441 Lyons Road
Coconut Creek, Florida 33073
USA

Telephone: (954) 946-2274
Fax: (954) 337-6424

Sales & General Information: info@repliweb.com
Documentation: docs@repliweb.com
Technical Support: <http://support.repliweb.com>
Website: <http://www.repliweb.com>

Table of Contents

1.	Introduction.....	1
2.	Security Rules.....	2
	Security Rules Parsing	3
3.	Users and Rules Management.....	4
	Defining Users	5
	Updating the Submit Command.....	7
	Managing Rules.....	8
4.	Examples.....	13
	User Configurations	13
	Mapping All Users to One User	13
	Rules Configurations	19
	Allowing Connection from the Web UI Only.....	19
	Allowing SSL-only connections:.....	22
	Allowing Backup & Restore in SSL mode:.....	23

1. Introduction

The RepliWeb User Account Proxy is a layer within the RepliWeb R-1 and RDS platforms that acts as both an incoming security reference monitor and as a User proxy.

NOTE: The samples provided in this doc are applicable to R-1 and RDS, using the respective console and command lines.

A system administrator can control R-1 and RDS operations on any system component (Controller, Satellite, Center, Edge) through the **Proxy Security Mechanism**.

Whenever a request for an R-1 and RDS operation is received, it activates a security check, which compares the details of the requested operation against a rule base. Based on the administrator-defined rules recorded in this file, the operation is approved or refused.

The Proxy Security Mechanism plays two major roles:

- It is an administrative tool, allowing administrators to control how users use R-1 and RDS and its related programs.
- It is a security tool, allowing administrators to control all incoming R-1 and RDS requests from outside.

The Proxy Security Mechanism serves here as a data transfer firewall, allowing remote users access without exposing any system account and password information.

To understand how the Proxy Security Mechanism carries out these functions, it is useful to know how it performs the security check.

For each requested operation, a number of parameters are examined during a security check. These include the requester's node, user name and network address, the local user name and password given for the operation, the type of operation or command, the affected files and directories, the time of day, and any special codes or identifying signs used in the operation.

Any of these properties can be used as criteria to determine if a given rule should apply to the operation. A matching rule can instruct the checking application to refuse or approve the requested operation.

The rules can also tell the application to modify the operation's properties, such as changing the local user account the operation is carried under.

Once a particular requested session has been approved, the action taken is to fork the child process that handles the request under the specified local user context defined in the security file.

This is the “Virtual User” functionality.

2. Security Rules

The Proxy Security Mechanism operates on the principal of Active Security: instead of passively relying on the system's built-in security measures, it actively takes any information it has on the requested operation and decides if it should be refused, approved or modified, based on any relevant rules defined in one or more security files.

Because of this, security is not based on what the remote user knows about a system (like `ftp` or `rsh` passive security), but on what the administrator actively allows to be done on the system through the security rule base.

This means that sensitive system information such as user account names or passwords don't have to be given to remote users or passed over the network.

The administrator decides exactly who is allowed to connect from where, what authentication process they must pass, and what exactly they will or will not be allowed to do.

Active Security can be used to limit access based on remote user's name, remote node's name, network address, and other identifiers. Complete sub-networks and user groups can be identified and restricted in a single rule.

The administrator can define Rules to divert remote users to specific local accounts, regardless of information they might possess.

By default, the security file in the R-1 and RDS evaluation kits allows all users with real username and passwords to have full access and control. Below is a brief description of each part of the rule followed by a short example of a secure set-up.

NOTE: The Security File `~rds/config/rw_security.cf` **must** have restricted permissions set on it (600 on UNIX and Administrator only on Windows) otherwise an error would be returned connection.

Security Rules Parsing

Rules comprise of 3 major parts:

- **WHO** is the User - this part includes information to match the user trying to access the server. This includes the requester's node, user name and network address, the local user name and password given for the operation, the type of operation or command, the files and directories affected, the time of day, etc.
- **WHAT** is the Rule – this part specifies if the rule accepts or denies the user.
- Is this the **LAST** Rule – As part of the rule definition, it is specified if to keep looking for other rules that match this user, or to stop the rule parsing and act upon this rule's specification. This is applied only if the user matches the requesting user's specification.

The security rule based is parsed in the following way:

1. The rules are parsed in an ascending order.
2. The user is compared against the first rule's specifications.
3. If the rule applies to this user:
 - a. The user is granted or denied access according to the rule's specification.
 - b. If this rule is marked "stop" – the user's access is granted or denied according to that rule. Otherwise, parsing of the rules continues to the next rule.
4. If the rule does not apply to this user, continue to the next rule.

NOTE: The Rule base is parsed such that later rules will overwrite and take precedence over earlier ones.

3. Users and Rules Management

The Console GUI - Manage option and the RepliWeb Topology Manager - RTM enable you to define virtual users and the rules to convert them to real users. It can be used on Windows systems only.

- **For RDS** - To use a virtual user between the **Controller** and a **Satellite**, you should connect to the **Satellite**. If you want to use a virtual user between your **Console** and **Controller**, connect to the **Controller**.
- **For R-1** - To use a virtual user between the **Center** and an **Edge**, you should connect to the **Edge**. If you want to use a virtual user between your **Console** and **Center**, connect to the **Center**.

The virtual user and the rules are defined on the machine accepting the connection. This way, the machine initiating the connection “knows” only virtual information and only virtual information is sent on the network. Real information never leaves the machine accepting the connection.

Defining Users

The Virtual Users tab enables you to define virtual users to convert them to real users. These users may be used for connection between the **Console** and **Center**.

Virtual users are defined on the machine accepting the connection. This way, the machine initiating the connection “knows” only virtual information and only virtual information is sent on the network. Real information never leaves the machine accepting the connection.

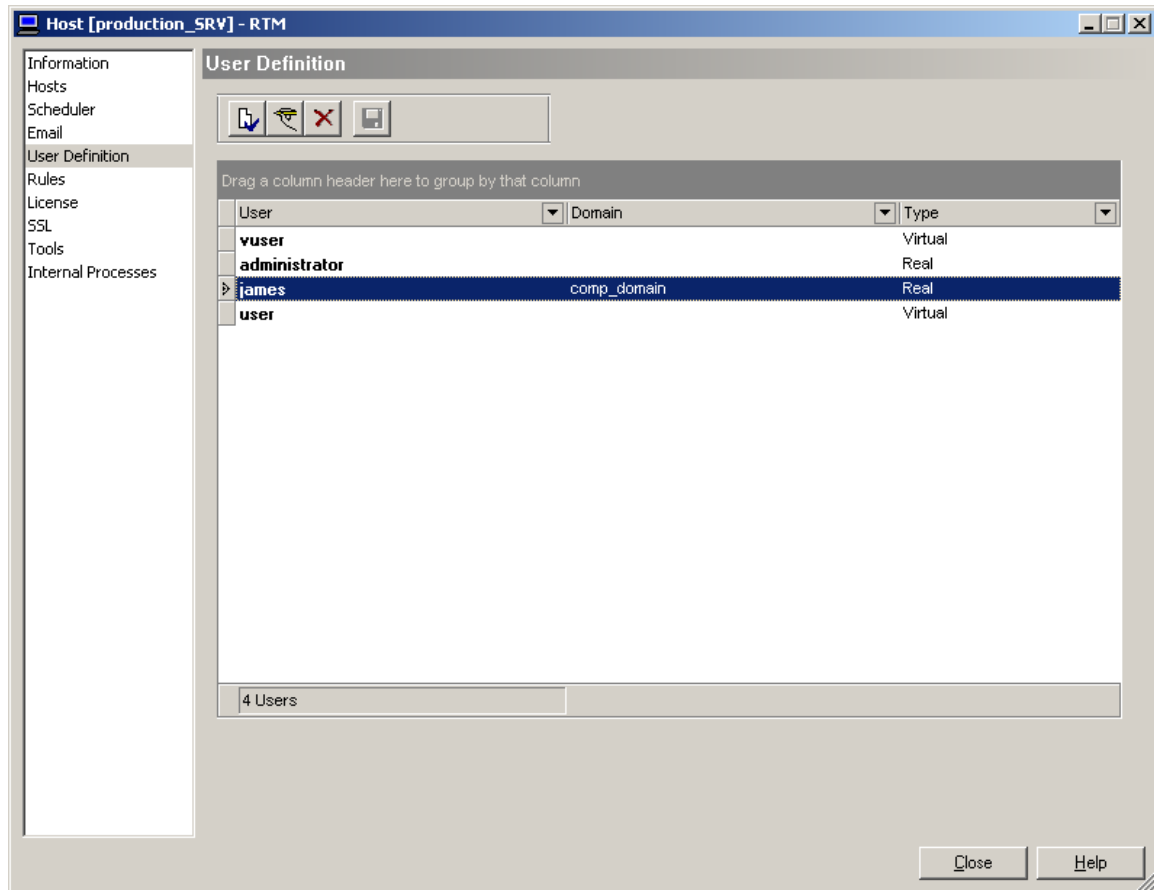
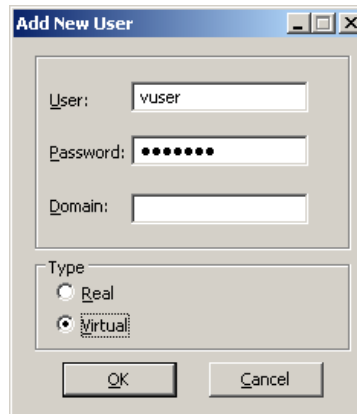


Figure 1: Define Virtual Users

1. Click the leftmost button to add a new user.



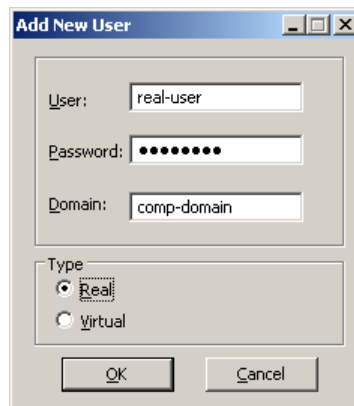
The screenshot shows a dialog box titled "Add New User". It contains three input fields: "User:" with the text "vuser", "Password:" with seven dots, and "Domain:" which is empty. Below these fields is a "Type" section with two radio buttons: "Real" (unselected) and "Virtual" (selected). At the bottom are "OK" and "Cancel" buttons.

Figure 2: Adding Virtual Users

2. Add the virtual user and virtual password. Leave the domain field blank.

NOTE: There is no virtual domain. If you put something there it will look for that user in a real domain.

3. Select the **Virtual** radio button and click **OK**.
4. Now add another user, this time the real user that the virtual user is translated to. Check the **Real** radio button and fill a real Domain:



The screenshot shows a dialog box titled "Add New User". It contains three input fields: "User:" with the text "real-user", "Password:" with seven dots, and "Domain:" with the text "comp-domain". Below these fields is a "Type" section with two radio buttons: "Real" (selected) and "Virtual" (unselected). At the bottom are "OK" and "Cancel" buttons.

Figure 3: Adding Real Users

5. Click the **Save** button.

Updating the Submit Command

Assuming that you have defined virtual users on an **R-1 Edge** or **RDS Satellite**, you can go back to your **submit command** on the **Console**, and change the user/password combination for the remote connection:

Instead of:

```
> r1 submit ... -user=real-user -password=xxx -domain=compdomain
```

you can now specify:

```
> r1 submit ... -user=vuser -password=vpass (← no domain)
```

Managing Rules

The Security Rules tab enables you to define rules that apply to real and virtual users. These rules apply for connecting from the **Console** to the **Center**.

Security rules are defined on the machine accepting the connection, as this is where access to real and virtual users is granted or denied. Here you define the connection between the virtual user and the real user.

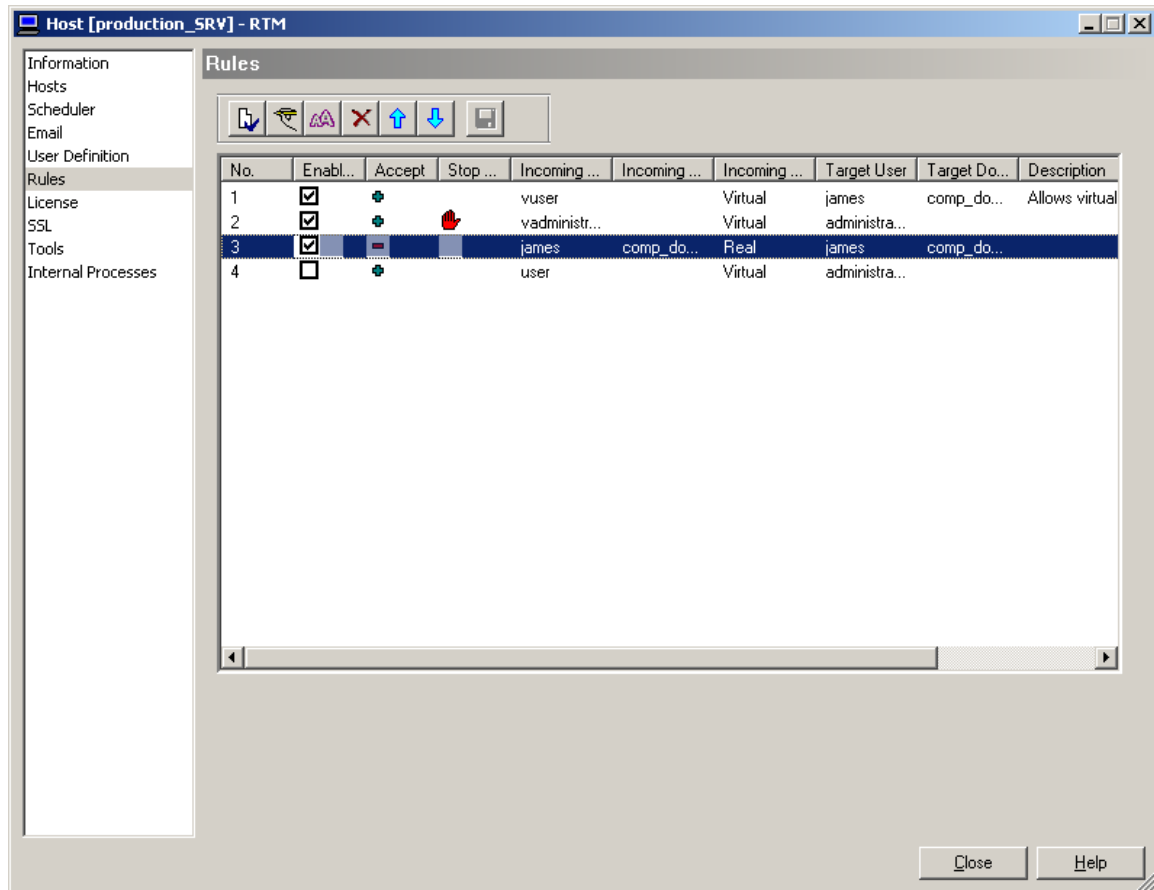


Figure 4: Security Rules Tab

To define a new security rule:

1. Click the leftmost button “**New Rule**” to add a new rule.

Figure 5: Adding a Rule

- **Enable Rule** – Specify if this rule is enabled or not. If this option is not selected the rule is not taken into account while evaluating a user.
- **Description** – Fill in a description of that rule. This field has no effect on the rule’s functionality.
- **Incoming User** - specify the user name performing the connection. This user name will be translated to a real user on the target machine. Specify if the incoming user is **Virtual** or not.
 - If the incoming user is a virtual user, you may define a virtual **domain** as well. The domain will be then used in the actual connection command.

NOTE: In UNIX, you can only define virtual users. No need to define real users to be used in the Rules Tab. In Windows, in order to map a virtual user to a real user, the real user must be defined in the User Definition tab as well.

- In a **Console → Center / Host connection**, the incoming user is the one used in the Console Connection screen.
- In a **Center → Edge connection**, the incoming user is the one used in the job definition.

- **SSL** - Specify if SSL is considered during the connection:
 - **With SSL** - The connection must be with SSL
 - **Without SSL** - The connection must be without SSL.
- **Action** - specify if the rule is “positive” – approve the user to connect (**Accept**), or “negative” – deny access to that user (**Reject**).
- **Transform To** - specify the real target user the **Incoming User** is translated to.
 - If applicable, specify **Domain**.

NOTE: If the virtual user was defined with a domain (a virtual one), you should also specify that domain name here.

This is a basic rule. As we defined only one user, all you have to do is click OK to say that the user “*vuser*”, will be examined as a virtual user and translated to the real user “*james*” from the domain “*comp_domain*”.

- **Stop Search** – Do not check that user using other rules. If the incoming user matches that rule, accept or deny according to that rule.
- **Advanced** – Rules may be further enhanced to tighten security and limit accessibility to R-1/RDS machines. These features describe the operating system environment from which the connection request is coming from.

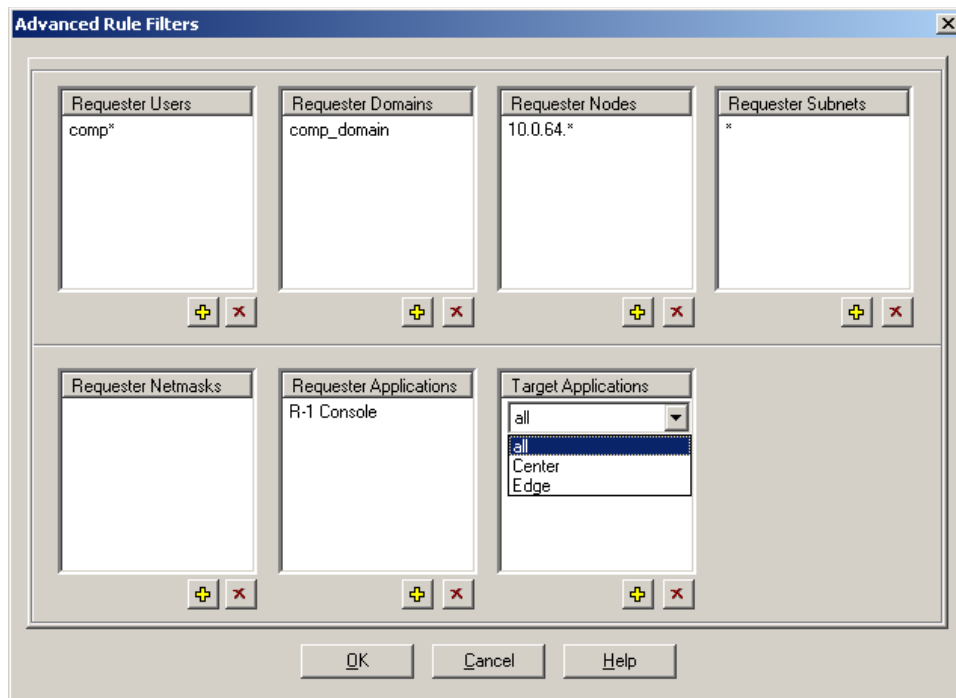


Figure 6: Advanced Rule Parameters

- **Requester Users** - Wildcard and multiple values are supported.
 - In a **Console → Controller / Center connection**, this is the ACTUAL ACCOUNT from which the R-1/RDS command came from, i.e. Windows or UNIX account, not the Console login.

- In a **Controller / Center → Satellite / Edge connection**, this is the user used in the Console login to the Controller / Center.
- **Requester Domains** – Wildcard and multiple values are supported.
 - In a **Console → Controller / Center connection**, this is the ACTUAL Windows domain from which the R-1/RDS command came from.
 - In a **Controller / Center → Satellite / Edge connection**, this is the domain of the user used in the Console login to the Controller / Center.
- **Requester Nodes** – The machine name from which the request comes from. Wildcard and multiple values are supported.
 - In a **Console → Controller / Center connection**, this is the network name of the Console machine.
 - In a **Controller / Center → Satellite / Edge connection**, this is the network name of the Controller / Center.
- **Requester Subnets** – The subnet from which the request comes from. Wildcard and multiple values are supported. 17.0.84.*- for example.
 - In a **Console → Controller / Center connection**, this is the subnet of the Console machine.
 - In a **Controller / Center → Satellite / Edge connection**, this is the subnet of the Controller / Center.
- **Requester Netmasks** – The netmask from which the request comes from. Wildcard and multiple values are supported. 255.255.255.0 - for example.
 - In a **Console → Controller / Center connection**, this is the netmask of the Console machine.
 - In a **Controller / Center → Satellite / Edge connection**, this is the netmask of the Controller / Center.
- **Requester Applications** – The application name from which the request comes from. Multiple values are supported, and ALL can be selected meaning the request can come from any of the listed applications. This field can have the following options:
 - Console (R-1 or RDS)
 - Command Line
 - API
 - Replication Job
 - Multicast Distribution
 - Backup
 - Restore
- **Target Applications** – The target application receiving the connection request. This field can have the following options:
 - R-1 Center / RDS Controller

- R-1 Edge / RDS Satellite

In the screen-shot above, only users that their name begins with “*comp*”, from domain “*comp_domain*”, and that are connecting from machines whose IP address begins with *12.0.76* are allowed to connect. Other users will not pass that rule and their connection request will be denied.

2. Click the **Save** button.
3. Defining a few rules, you can determine the order in which the rules are applied when a user tried to connect to the machine. To update the location of a rule, right-click the rule, and in the floating menu select the **Move** option. A window will open, enabling to move the rule up and down between the existing rules.

4. Examples

This chapter provides examples of mapping users and delegating application access.

User Configurations

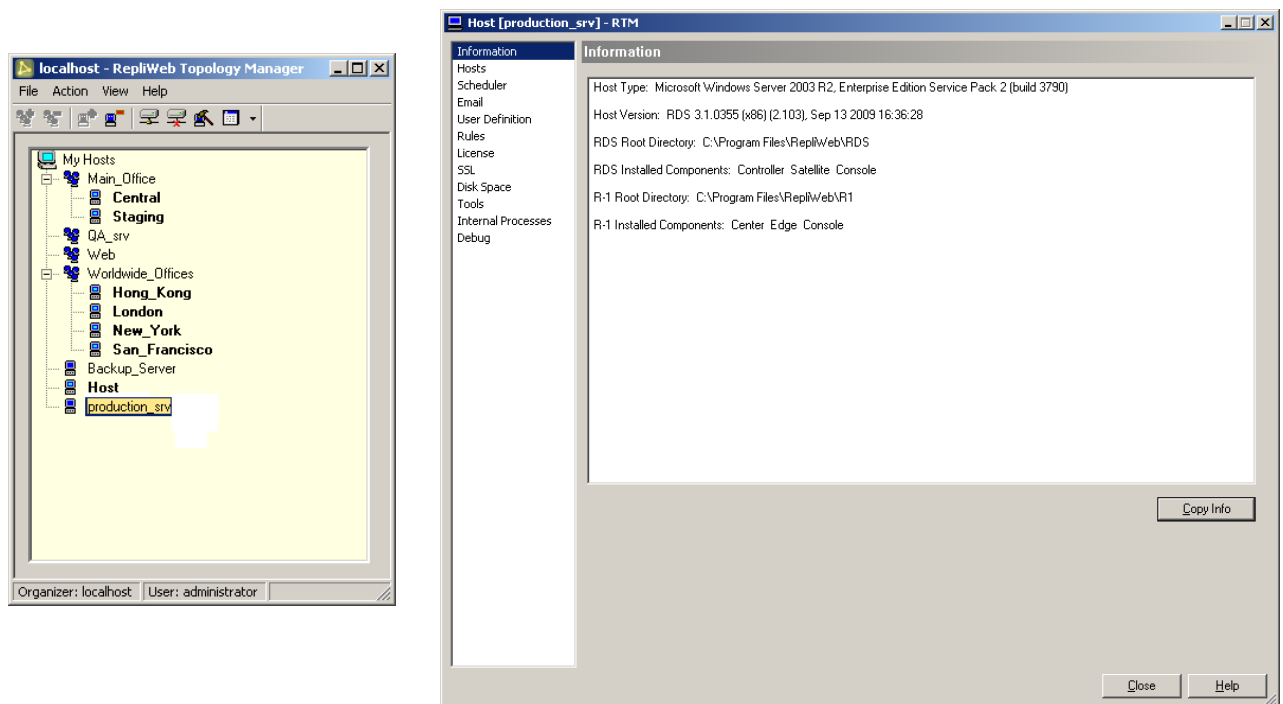
Mapping All Users to One User

A Linux Team Manager would like to map all incoming Web users to user `web_account` for a specific Server.

This can be achieved in two ways:

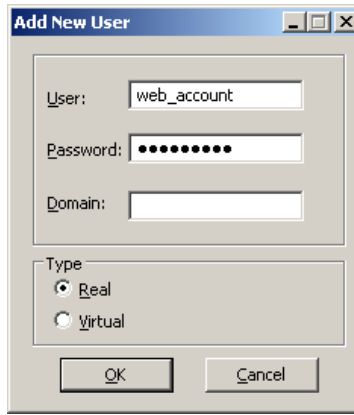
1. Map all **real** users to the Web Account user `web_account`. This way all users continue to use their own user name and password, but processes on that server run as `web_account`.
2. Create a **virtual** account to be used by all users while connecting, and map it to the Web account user on the server.

In the RTM console, double click the Edge to manage. Enter the username and password in the prompt. To edit the security configuration on Linux, connect as `root`.



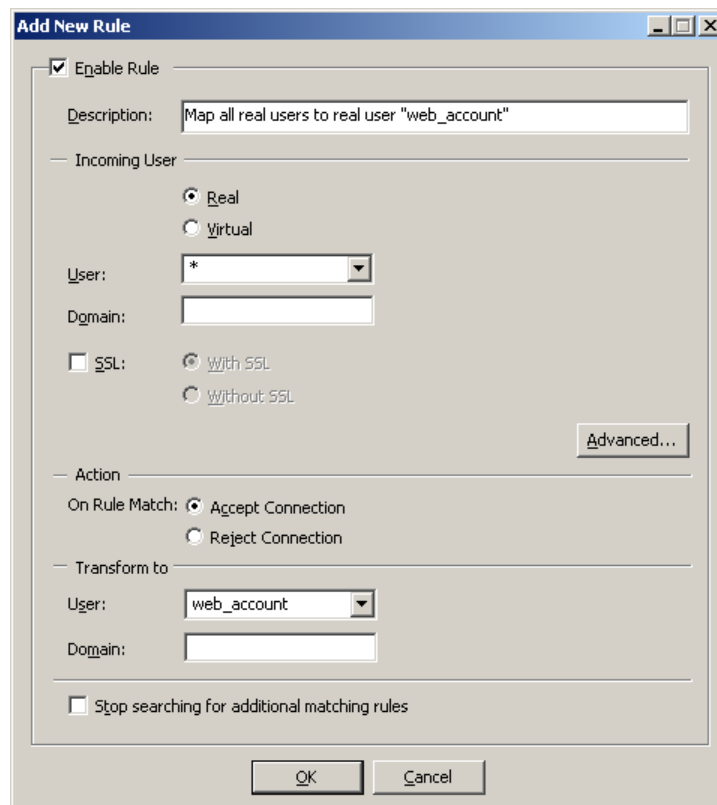
Mapping all real users to the Web Account user web_account

1. If using Windows, the real user `web_account` has to be added in the **User Definition** tab as a Real user.



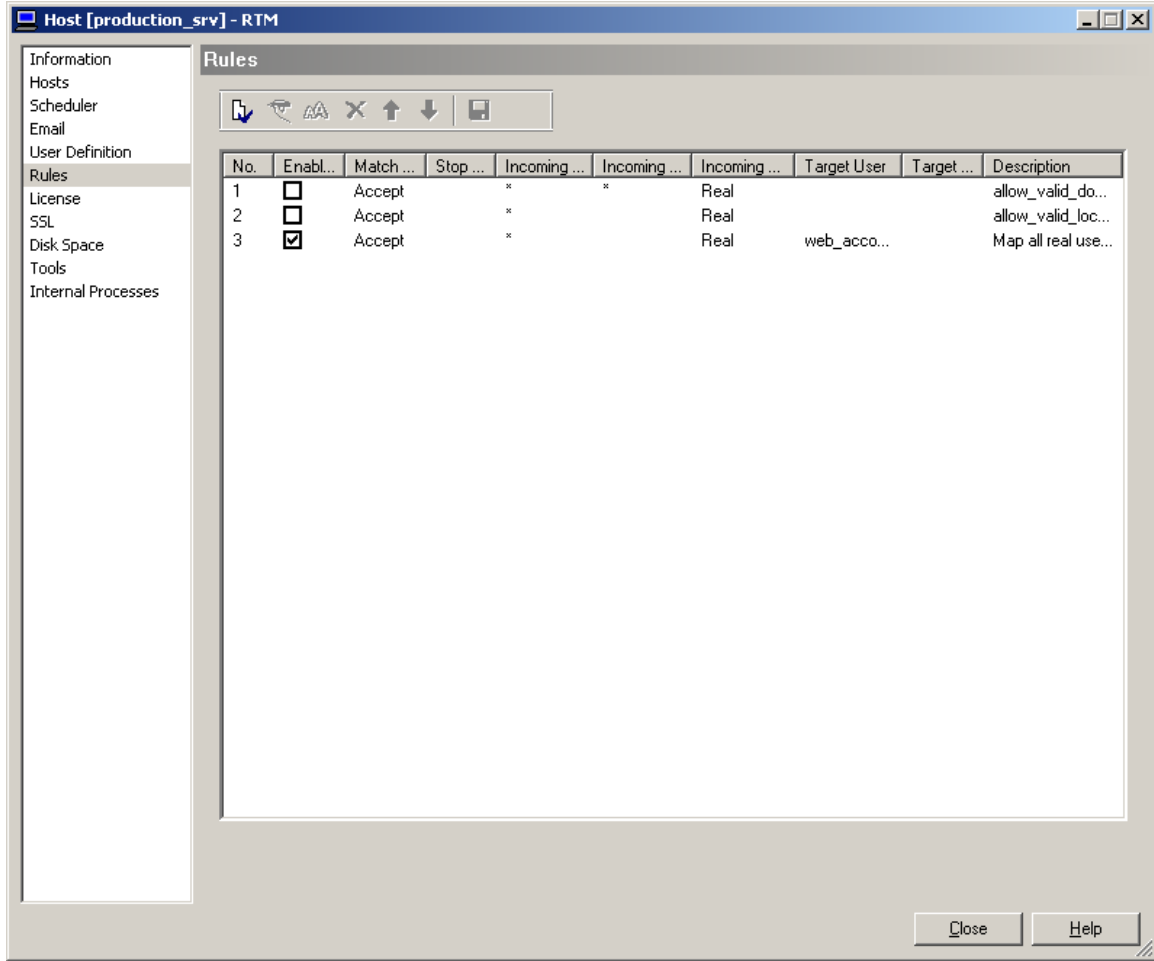
The 'Add New User' dialog box is shown. It has a title bar with standard window controls. The main area contains three input fields: 'User' with the text 'web_account', 'Password' with a masked field of dots, and 'Domain' which is empty. Below these is a 'Type' section with two radio buttons: 'Real' (selected) and 'Virtual'. At the bottom are 'OK' and 'Cancel' buttons.

2. Under the **Rules** tab, create a rule that maps all incoming users to user `web_account`. All access to that server will be done using real system users and passwords, but all processes will be transformed to run under the user context of the `web_account` user.



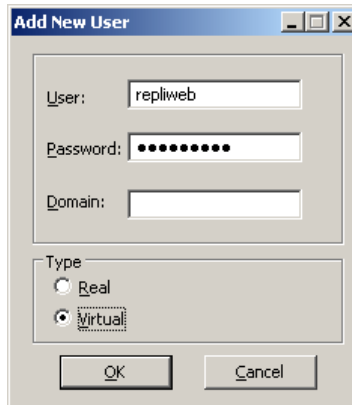
The 'Add New Rule' dialog box is shown. It has a title bar with standard window controls. The main area contains several sections: 'Enable Rule' (checked), 'Description' (text: 'Map all real users to real user "web_account"'), 'Incoming User' (radio buttons for 'Real' and 'Virtual', 'Real' selected; 'User' dropdown set to '*', 'Domain' empty), 'SSL' (checkbox unchecked, radio buttons for 'With SSL' and 'Without SSL'), 'Action' (radio buttons for 'Accept Connection' and 'Reject Connection', 'Accept Connection' selected), 'Transform to' (dropdown for 'User' set to 'web_account', 'Domain' empty), and 'Stop searching for additional matching rules' (checkbox unchecked). At the bottom are 'OK' and 'Cancel' buttons.

3. Also, edit the first two rules to reject access from any user account.



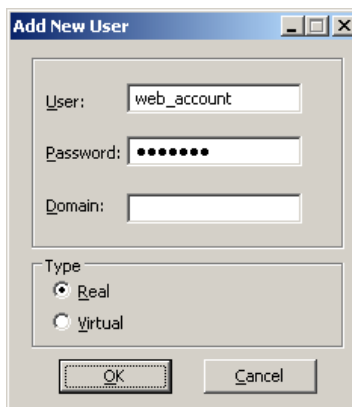
Mapping a Virtual user to the Web Account user `web_account`.

1. Under the **User Definition** tab, create a new virtual user.



The screenshot shows the 'Add New User' dialog box. The 'User' field contains 'repliweb', the 'Password' field contains seven dots, and the 'Domain' field is empty. Under the 'Type' section, the 'Virtual' radio button is selected, and the 'OK' button is highlighted.

2. If using Windows, the real user `web_account` has to be added in the **User Definition** tab as a **Real** user.



The screenshot shows the 'Add New User' dialog box. The 'User' field contains 'web_account', the 'Password' field contains seven dots, and the 'Domain' field is empty. Under the 'Type' section, the 'Real' radio button is selected, and the 'OK' button is highlighted.

3. In the **Rules** tab, create a rule that maps the virtual `repliweb` user to user `web_account`. All access to that server will be done using that virtual user, but all processes will be transformed to run under the context of the `web_account` user.

Update Rule

Enable Rule

Description: Map virtual user "repliweb" to real user "web_account"

Incoming User

Real

Virtual

User: repliweb

Domain:

SSL: With SSL Without SSL

Advanced...

Action

On Rule Match: Accept Connection Reject Connection

Transform to

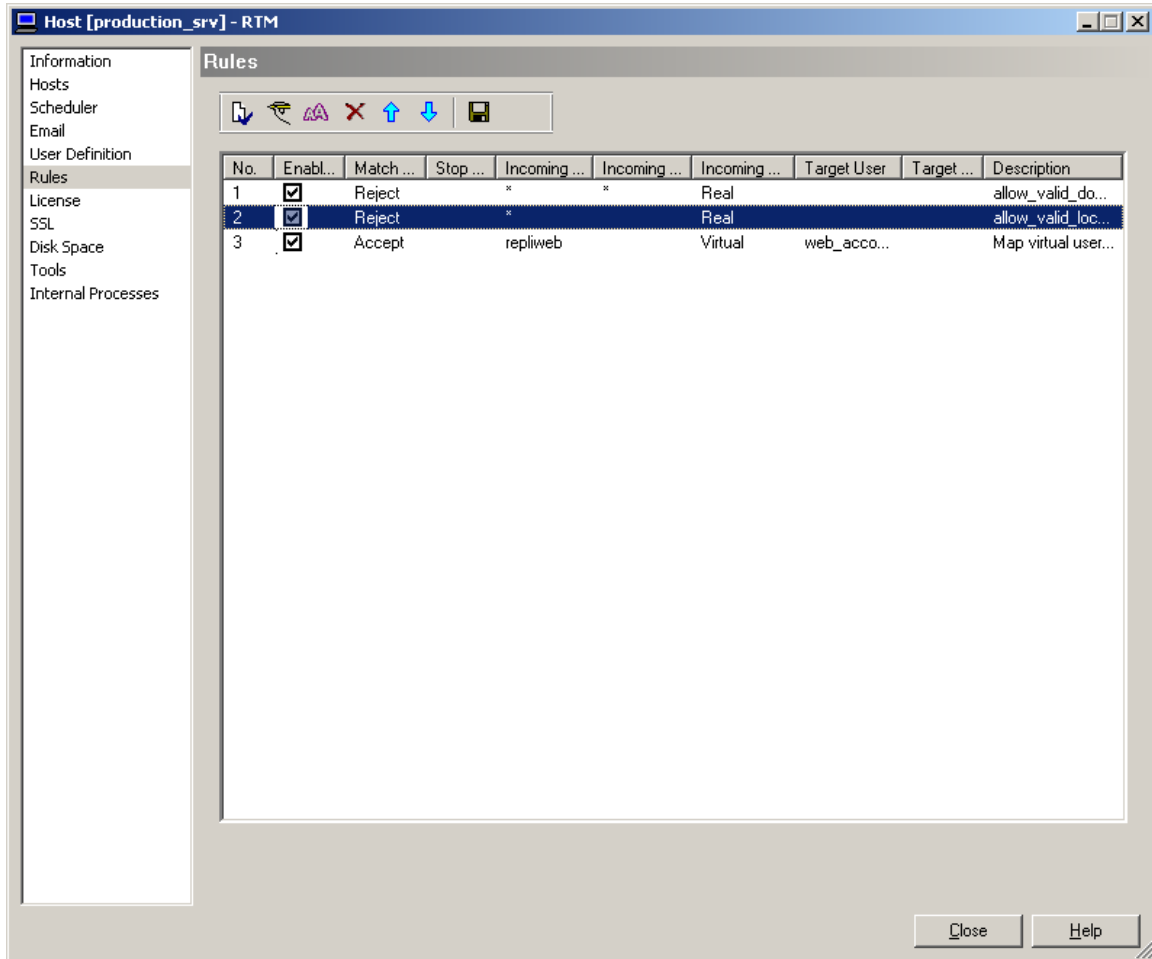
User: web_account

Domain:

Stop searching for additional matching rules

OK Cancel

4. Also, edit the first two rules to reject access from any user account.




Rules Configurations

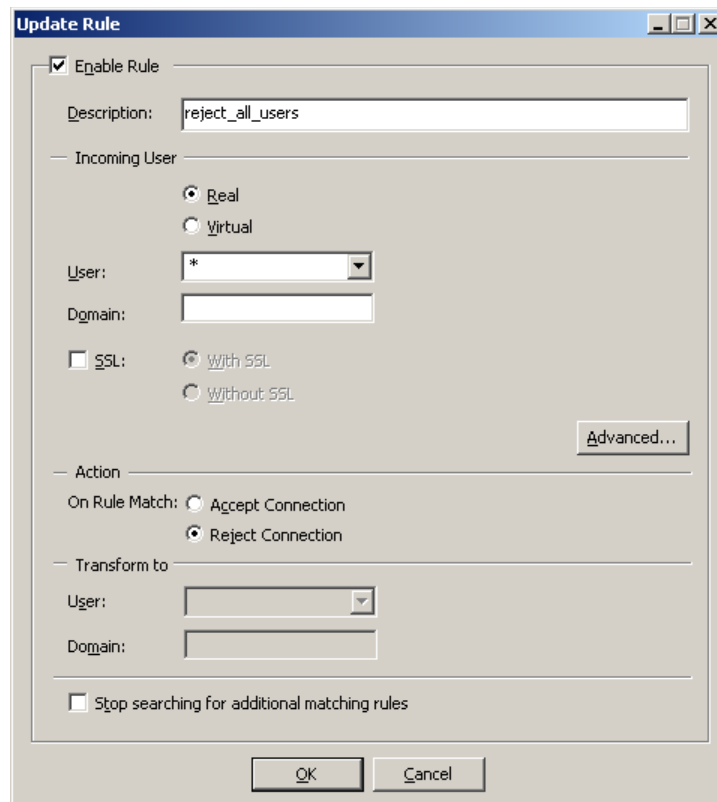
Allowing Connection from the Web UI Only

The following example shows how to enable access to users connecting from the Web UI while rejecting a connection from all other interfaces.

NOTE: Make sure to disable any existing rules (by unchecking each rule's **Enable Rule** checkbox) before performing this procedure.

NOTE: The procedure below assumes that any existing rules have been disabled.

1. Click **New Rule**  to add a new rule that rejects access from all local users.
 - a. In the **Incoming User** area, select the **Real** option and enter an asterisk (*) in the **User** field.
 - b. In the **Action** area, select the **Reject Connection** option.



The screenshot shows the 'Update Rule' dialog box with the following configuration:

- Enable Rule
- Description: reject_all_users
- Incoming User:
 - Real
 - Virtual
 - User: *
 - Domain: (empty)
- SSL:
 - With SSL
 - Without SSL
- Advanced... (button)
- Action:
 - On Rule Match: Accept Connection
 - Reject Connection
- Transform to:
 - User: (empty)
 - Domain: (empty)
- Stop searching for additional matching rules
- OK (highlighted) | Cancel

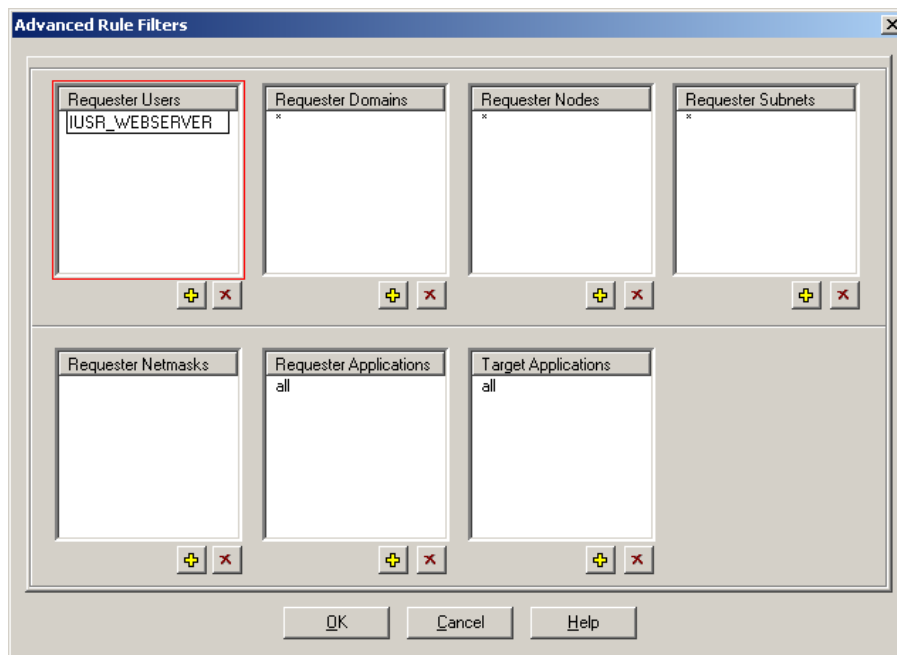
- c. Click **OK**.
2. If you are using a domain environment, add another rule that rejects domain users.
 - a. In the **Incoming User** area, select the **Real** option and enter an asterisk (*) for both the **User** and **Domain** fields.

- b. In the **Action** area, select the **Reject Connection** option.
3. Add another rule that enables access to the Center for users connecting from a specific Web UI machine. For example, machine: `WebServer`.
 - a. In the **Incoming User** area, select the **Real** option and enter an asterisk (*) as the **User**.
 - b. In the **Action** area, make sure that the **Accept Connection** option is selected.
 - c. Click the **Advanced** button, the **Advanced Rule Filters** window appears.
 - d. In **Requester Users**, remove the default asterisk (*) and any existing users, and enable Web UI users by entering: **IUSR_<MACHINE NAME>**

where **<MACHINE NAME>** is the machine running the IIS that you are connecting to.

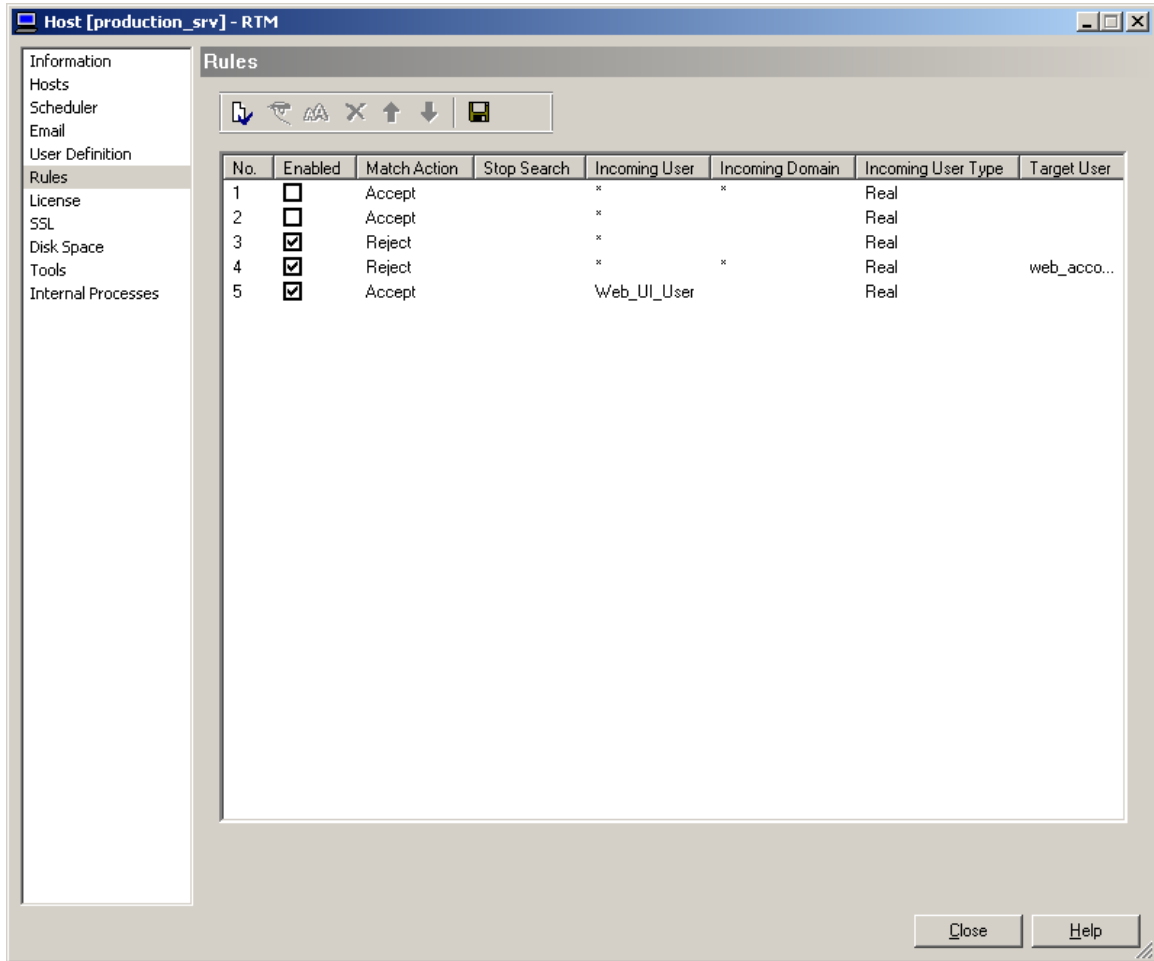
NOTE: The "IUSR_" prefix is mandatory.

For example, IUSR_WEBSERVER:



4. Click **OK**.

The **Security Rules** tab should look as follows:




Allowing SSL-only connections:

This rule allows connections in SSL mode only while rejecting non-SSL connections.

NOTE: If Backup & Restore is needed, make sure the **Allow backup and restore** security rules are enabled and appear first in the Center Management's Security Rules list. For more information on these rules, refer to the next example.

To allow an SSL-only connection:


1. Click **New Rule**  to add a new rule.
2. In the **Description** field, enter a proper description, such as “**Allow ssl connection only**”.
3. In the **Incoming User** area, select the **Real** option and enter an asterisk (*) for the **User** field.
4. Select the **SSL** checkbox and make sure **With SSL** is selected.
5. In the **Action** area, select the **Accept Connection** option.
6. Click **OK**.

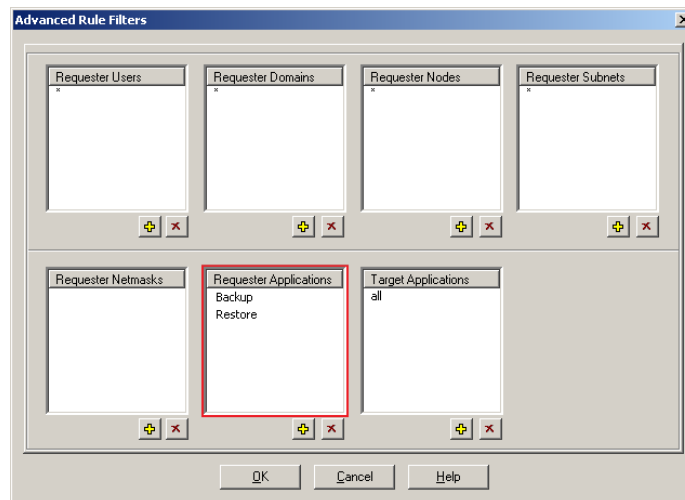
Allowing Backup & Restore in SSL mode:

In environments that require an SSL connection, the following two rules need to be created to enable Backup & Restore to run.

NOTE: For these rules to work properly, make sure they are enabled and appear first in the Rules list.


To allow Backup & Restore for all real domain users:

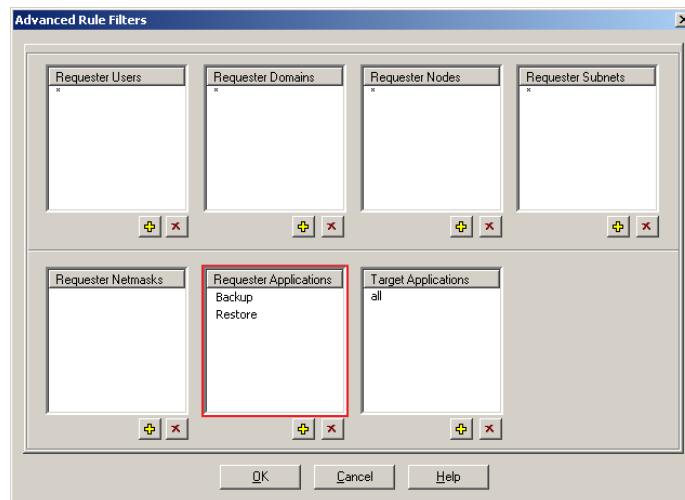
1. Click **New Rule**  to add a new rule.
2. In the **Description** field, enter a proper description, such as “**Allow backup and restore access to domain users**”.
3. In the **Incoming User** area, select the **Real** option and enter an asterisk (*) for both the **User** and **Domain** fields.
4. In the **Action** area, select the **Accept Connection** option.
5. Click the **Advanced** button, the **Advanced Rule Filters** window appears.
 - a. In **Requester Applications**, remove the **all** entry and add the following two entries: **Backup** and **Restore**, as follows:



- b. Click **OK**.
6. Select the **Stop searching for additional rules** checkbox.
 7. Click **OK**.

To allow Backup & Restore for all real local users:

1. Click **New Rule**  to add a new rule.
2. In the **Description** field, enter a relevant description, such as “**Allow backup and restore access to local users**”.
3. In the **Incoming User** area, select the **Real** option and enter an asterisk (*) for the **User** field.
4. In the **Action** area, select the **Accept Connection** option.
5. Click the **Advanced** button, the **Advanced Rule Filters** window appears.
 - a. In **Requester Applications**, remove the **all** entry and add the following two entries: **Backup** and **Restore**, as follows:



- b. Click **OK**.
6. Select the **Stop searching for additional rules** checkbox.
 7. Click **OK**.

For any additional information, contact us at support.repliweb.com