

Security Server Setting Guide

This manual is currently reference document. Officially, please check the Japanese one.

Contents

1. Introduction	3
1.1 Target Audience	4
1.2 Skill set.....	4
1.3 PlanetCross Security Server	4
1.4 PlanetCross Concepts	5
2. User Management.....	7
2.1 User Roles	7
2.2 Managing the Users.....	7
2.2.1 Adding User.....	7
2.2.2 Setting Permissions	8
2.2.3 Deleting Permissions	8
2.2.4 Deleting User	8
3. Security Server Clients.....	9
3.1 Security Server Clients Status	9
3.2 Adding a Security Server Client.....	10
3.3 Configuring a Signing Key and Certificate for a Security Server Client.....	13
3.4 Registering a Security Server Client in the PlanetCross Governing Authority.....	14
3.4.1 Registering a Security Server Client.....	14
3.5 Deleting a Client from the Security Server	16
3.5.1 Unregistering a Client	16
3.5.2 Deleting a Client.....	18
3.6 Registering multiple members to Security Server	20
3.6.1 In case use owe security server with multiple organization.....	20
4. Security Tokens, Keys, and Certificates.....	22
4.1 Availability States of Security Tokens, Keys, and Certificates.....	22
4.2 Registration States of Certificates	22
4.2.1 Registration States of the Signing Certificate	22
4.2.2 Registration States of the Authentication Certificate	23
4.3 Validity States of Certificates	24
4.4 Activating and Disabling the Certificates	25
4.5 Configuring and Registering an Authentication key and Certificate	26
4.6 Deleting a Certificate	26
4.6.1 Unregistering an Authentication Certificate	26
4.6.2 Deleting a Certificate or a certificate Signing Request notice	27
4.7 Deleting a Key.....	28
5. Setting a Service	29
5.1 PlanetCross Service	29
5.2 Adding a WSDL	29
5.3 Refreshing a WSDL	31
5.4 Enabling and Disabling a WSDL	32
5.5 Changing the Address of a WSDL.....	34
5.6 Deleting a WSDL	35
5.7 Changing the Parameters of a Service	36
6. Access Rights	38
6.1 Changing the Access Rights of a Service	38
6.2 Adding a Service Client.....	41
6.3 Changing the Access Rights of a Service Client	44
6.4 Local Access Right Groups	47
6.5 Adding a Local Group	48
6.6 Displaying and Changing the Members of a Local Group	50

6.7 Changing the description of a Local Group	54
6.8 Deleting a Local Group	55
7. Communication with the Client Information Systems	57
8. System Parameters	64
8.1 Managing the Configuration Anchor	64
8.2 Managing the Timestamping Services	65
8.3 Changing the Internal TLS Key and Certificate	67
9. Message Log	70
9.1 Changing the Configuration of the Message Log	70
9.1.1 Common parameters	70
9.1.2 Timestamping parameters	71
9.1.3 Archiving parameters	71
9.2 Setting the message log acquisition level and size	71
9.2.1 Setting the message log acquisition level	71
9.2.2 Setting the message log size	72
9.3 Transferring the Archive Files from the Security Server	72
9.4 Using a Remote Database	73
10. Audit Log	75
10.1 Changing the Configuration of the Audit Log	76
10.2 Archiving the Audit Log	76
Appendix A. Subsystem Naming Convention Best Practices	77
A.1 About the subsystem	77
A.2 The subsystem naming guideline	77
A.3 Allowable characters for subsystem names	77
Appendix B. Periodic backup of security server, using CRON	78
B.1 Backup script	78
B.2 Setting a Cron	78
B.3 RSYNC to remote backup storage server	79
B.3.1 Backups storage server configuration	79
B.3.2 Security server configuration	80
Appendix C. Message logs archiving configuration	81
C.1 Message logs configuration file	81
C.2 Parameters	81
C.3 Archived message logs transferring configuration	82
C.3.1 Archive server configuration	82
C.3.2 Security server configuration	83
C.4 Recommendations for production message logs archiving	84
Appendix D. Setting for big query	85
D.1 Enable swap	85
D.2 Change proxy Xmx	85
D.3 Turn off SOAP body logging	86
D.4 Raise limit for SOAP body logging	86
D.5 Combination of settings and test result	87
Revision History	88

1. Introduction

About trademark

- "Amazon Web Services", the "Powered by Amazon Web Services" logo and "AWS" are trademarks of Amazon.com, Inc. or its affiliates in the United States and/or other countries.
- UNIX is a registered trademark of The Open Group in the United States and in other countries.
- Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.
- PostgreSQL is trademark or registered trademark of PostgreSQL of the U.S. in the U.S. and/or other countries.
- X-Road® is a registered trademark of the Estonian Information System Authority (RIA).
- Planetway, PlanetCross are trademarks of Advanced Planetway Japan K.K.
- All other brand or product names may be trademarks or registered trademarks of their respective companies or organizations.

1.1 Target Audience

This Security Server setting guide is aimed at PlanetCross security server system administrators for installing, operating and maintaining PlanetCross software.

1.2 Skill set

This document is intended for readers with a moderate knowledge of Linux server management, computer networks, and the PlanetCross working principles.

1.3 PlanetCross Security Server

The main function of a security server is to mediate requests in a way that preserves their evidential value.

The security server is connected to the public Internet from one side and to the information system within the organization's internal network from the other side. In a sense, the security server can be seen as a specialized application-level firewall that supports the SOAP protocol; hence, it should be set up in parallel with the organization's firewall, which mediates other protocols.

The security server is equipped with the functionality needed to secure the message exchange between a client and a service provider.

- Messages transmitted over the public Internet are secured using digital signatures and encryption.
- The service provider's security server applies access control to incoming messages, thus ensuring that only those users that have signed an appropriate agreement with the service provider can access the data.

To increase the availability of the entire system, the service user's and service provider's security servers can be set up in a redundant configuration as follows.

- One service user can use multiple security servers in parallel to perform requests.
- If a service provider connects multiple security servers to the network to provide the same services, the requests are load-balanced between the security servers.
- If one of the service provider's security servers goes offline, the requests are automatically redirected to other available security servers.

The security server also depends on a central server, which provides the global configuration.

1.4 PlanetCross Concepts

- **Global configuration**

A technical solution, through which PlanetCross governing authority regulates participants of PlanetCross. Global configuration consists of XML-files, which are downloaded periodically from the central server of PlanetCross governing authority by security servers. Global configuration includes following information:

- the addresses and public keys of trust anchors (certification service CAs and time stamping services);
- the public keys of intermediate CAs;
- the addresses and public keys of OCSP services (if not already available through the certificates' *Authority Information Access* extension);
- information about PlanetCross members and their subsystems;
- the addresses of the members' security servers registered in PlanetCross;
- information about the security servers' authentication certificates registered in PlanetCross;
- information about the security servers' clients registered in PlanetCross;
- information about global access rights groups;
- PlanetCross system parameters.

- **Member class**

identifier, that is identified by the PlanetCross governing authority and that uniquely identifies members with similar characteristics. All members with the same member class must be uniquely identifiable by their member codes.

- **Member code**

identifier, that uniquely identifies an PlanetCross member within its member class. The member code remains unchanged during the entire lifetime of the member.

- **Security Server client**

a member or a subsystem of a member, whose relation with the security server is registered in PlanetCross governing authority and who can use the security server on behalf of a member to exchange data on PlanetCross.

- **Security Server owner**

a member responsible for security server and creation of a secure data exchange channel.

Subsystem represents a part of a PlanetCross member's information system. PlanetCross members must declare parts of its information system as subsystems to use or provide PlanetCross services.

- The access rights of an PlanetCross members' subsystems are independent – access rights given to one subsystem do not affect the access rights of the members' other subsystems.
- Services provided by a subsystem are independent of the services provided by the members' other subsystems.

To sign the messages sent by a subsystem when using or providing PlanetCross services, the signing certificate of the member that manages the subsystem is used. A PlanetCross member can associate several different subsystems with one security server, and one subsystem can be associated with several security servers.

- **PlanetCross certificate**

Issued by a certified service provider approved by the PlanetCross governing authority. A PlanetCross certificate is as follows:

- **Signature certificate** - qualified certificate of e-stamp issued by certification service provider approved on PlanetCross and bound to a member, used for verification of the integrity of mediated messages and association of the member with the message.
- **Authentication certificate** - qualified certificate of e-stamp issued by certification service provider approved on PlanetCross and bound to security server, certifying authenticity of security server and used for authentication of security servers upon establishment of connection between security servers. Upon establishment of connection, it is checked from global configuration, if the security server trying to establish connection has registered the used authentication certificate in PlanetCross governing authority (i.e. the used authentication certificate is bound to the ID of security server).

- **PlanetCross instance**

identifier, that uniquely identifies the PlanetCross instance in the PlanetCross Network.

- **PlanetCross member**

participant of PlanetCross entitled to exchange data/messages on PlanetCross.

- **PlanetCross message**

Data set meeting profile description and service description required by PlanetCross governing authority. Messages are divided into requests and responses.

2. User Management

2.1 User Roles

Security servers support the following user roles:

- **Security Officer** (xroad-security-officer) is responsible for the application of the security policy and security requirements, including the management of key settings, keys, and certificates.
- **Registration Officer**(xroad-registration-officer) is responsible for the registration and removal of security server clients.
- **Service Administrator**(xroad-service-administrator) manages the data of and access rights to services
- **System Administrator**(xroad-system-administrator) is responsible for the installation, configuration, and maintenance of the security server.
- **Security Server Observer**(xroad-securityserver-observer) can view the status of the security server without having access rights to edit the configuration. This role can be used to offer users read-only access to the security server admin user interface.

One user can have multiple roles and multiple users can be in the same role. Each role has a corresponding system group, created upon the installation of the system.

Henceforth each applicable section of the guide indicates, which user role is required to perform a particular action. For example:

Access rights: **Security Officer**

If the logged-in user does not have a permission to carry out a particular task, the button that would initiate the action is hidden (and neither is it possible to run the task using its corresponding keyboard combinations or mouse actions). Only the permitted data and actions are visible and available to the user.

2.2 Managing the Users

User management is carried out on command line in root user permissions.

2.2.1 Adding User

To add a new user, enter the command:

```
$ sudo adduser username
```

2.2.2 Setting Permissions

To grant permissions to the user you created, add it to the corresponding system groups, for example:

```
$ sudo adduser username xroad-security-officer
$ sudo adduser username xroad-registration-officer
$ sudo adduser username xroad-service-administrator
$ sudo adduser username xroad-system-administrator
$ sudo adduser username xroad-securityserver-observer
```

Settings are applied only after restart of the xroad-jetty service.

2.2.3 Deleting Permissions

To remove a user permission, remove the user from the corresponding system group, for example:

```
$ sudo deluser username xroad-security-officer
```

User permissions are applied only after restart of the xroad-jetty service.

2.2.4 Deleting User

To remove a user, enter:

```
$ sudo deluser username
```


3. Security Server Clients

Important	To use or provide PlanetCross services, a security server client needs to be certified by a certification service provider approved by the PlanetCross governing authority, and the association between the client and the security server used by the client must be registered at the PlanetCross governing authority.
------------------	--

This section describes managing Security Server clients.

【Note】




This section does not address managing the owner to a security server. The owner's information has been already added to the security server upon the installation, and registered upon the security server's registration. The owner's registration status can be looked up by selecting Security Server Clients on the Configuration menu. The security server's owner is displayed in bold. Before the registration of the security server, the owner is in the "Saved" state and after the completion of the registration process, in the "Registered" state.



The registration of the security server's owner does not extend to the owner's subsystems. The subsystems must be registered as individual clients.

Please refer to 『Security Server Installation Guide』 for these details.

3.1 Security Server Clients Status

The security server distinguishes between the following client states.

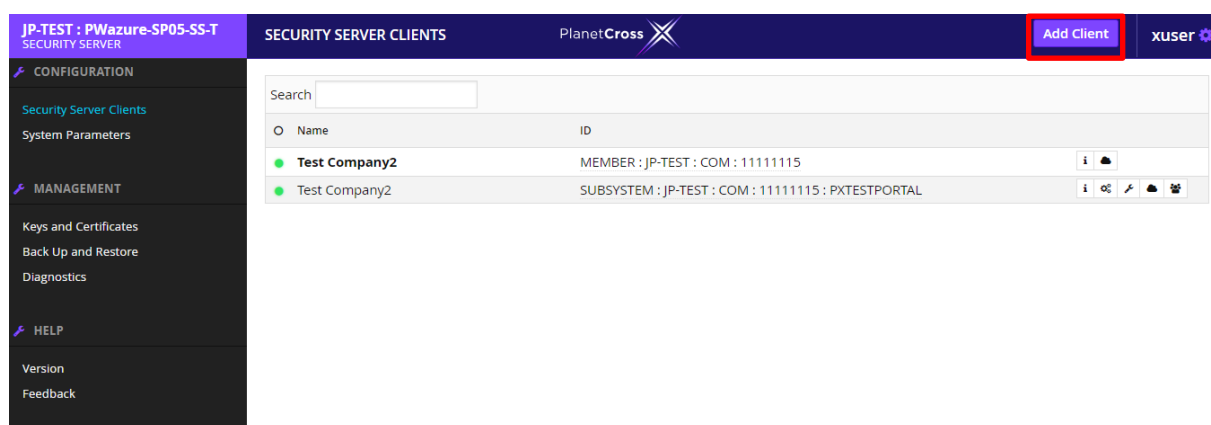
Status	Explanation
 Saved	The client's information has been entered and saved into the security server's configuration, but the association between the client and the security server is not registered in the PlanetCross governing authority. (If the association is registered in the central server prior to the entry of data, the client will move to the "Registered" state upon data entry.) From this state, the client can move to the following states: <ul style="list-style-type: none"> • "Registration in progress" : if a registration request for the client is submitted from the security server; • "Deleted" : if the client's information is deleted from the security server configuration.
 Registration in progress	A registration request for the client is submitted from the security server to the central server, but the association between the client and the security server is not yet approved by the PlanetCross governing authority. From this state, the client can move to the following states: <ul style="list-style-type: none"> • "Registered", if the association between the client and the security server is approved by the PlanetCross governing authority; • "Deletion in progress", if a client deletion request is submitted from the security server.
 Registered	The association between the client and the security server has been approved in the PlanetCross governing authority. In this state, the client can provide and use PlanetCross services (assuming all other prerequisites are fulfilled). From this state, the client can move to the following states: <ul style="list-style-type: none"> • "Global error" : if the association between the client and the security server has been revoked by the PlanetCross governing authority; • "Deletion in progress" : if a client deletion request is submitted from the security server.

Status	Explanation
 Global error	The association between the client and the security server has been revoked in the central server. From this state, the client can move to the following states: <ul style="list-style-type: none"> • "Registered" : if the association between the client and the security server has been restored in the central server (e.g., the association between the client and the security server was lost due to an error); • "Deleted" : if the client's information is deleted from the security server's configuration.
 Deletion in progress	A client deletion request has been submitted from the security server. From this state, the client can move to the following state: <ul style="list-style-type: none"> • "Deleted" : if the client's information is deleted from the security server's configuration.

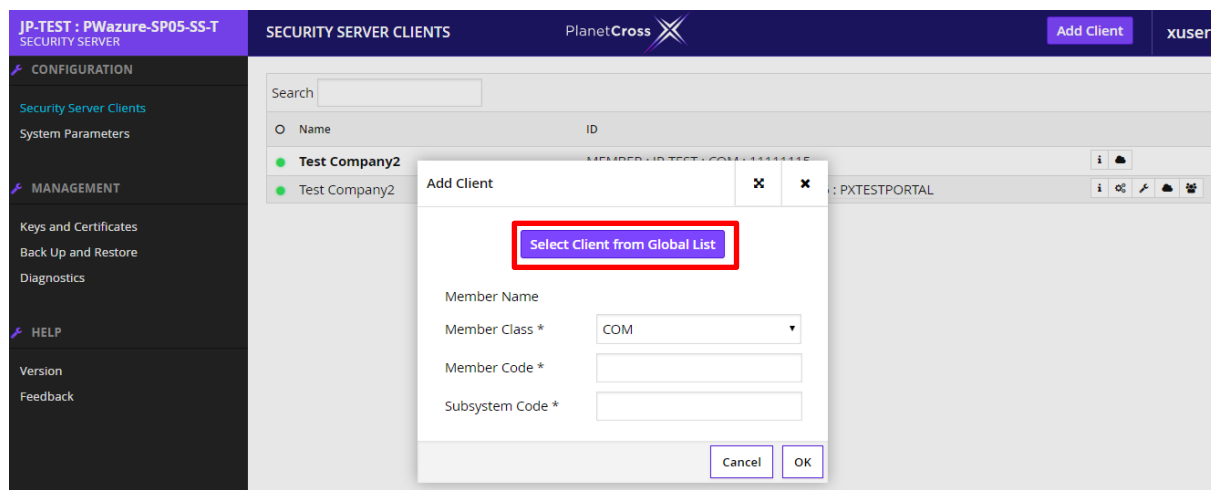
3.2 Adding a Security Server Client

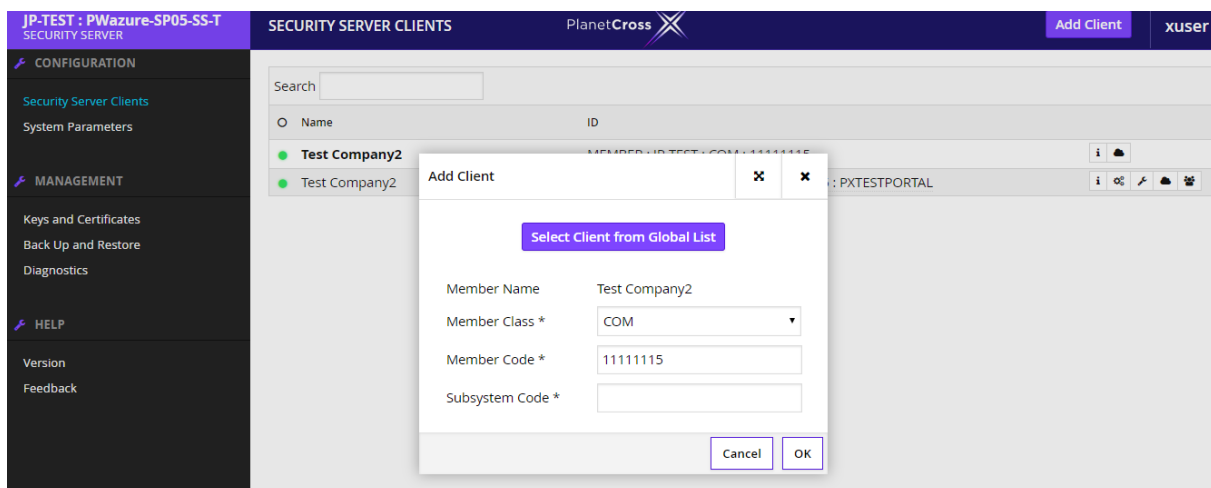
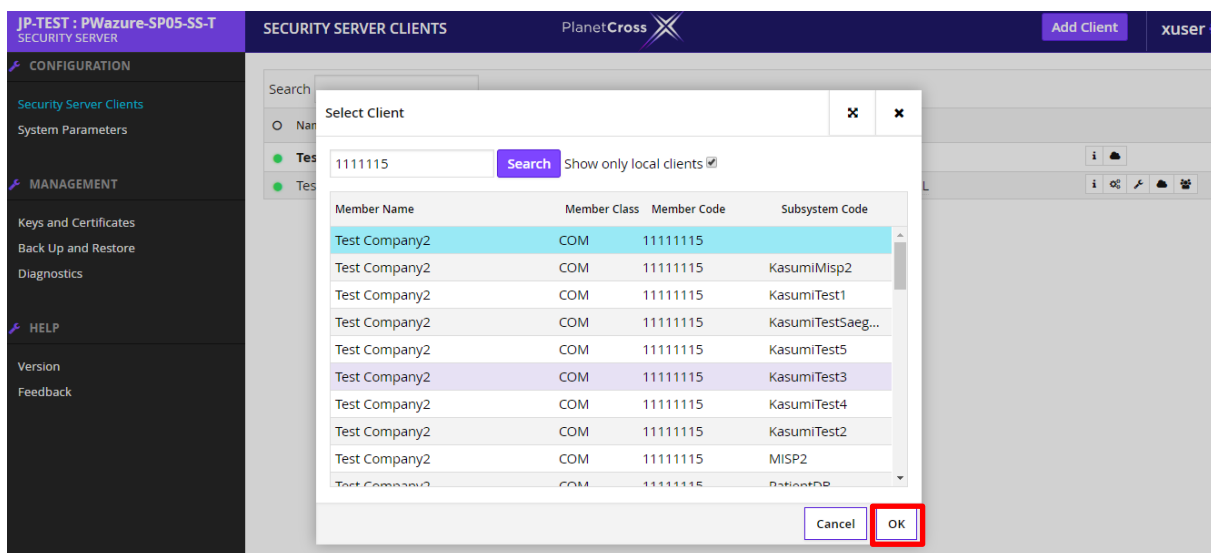
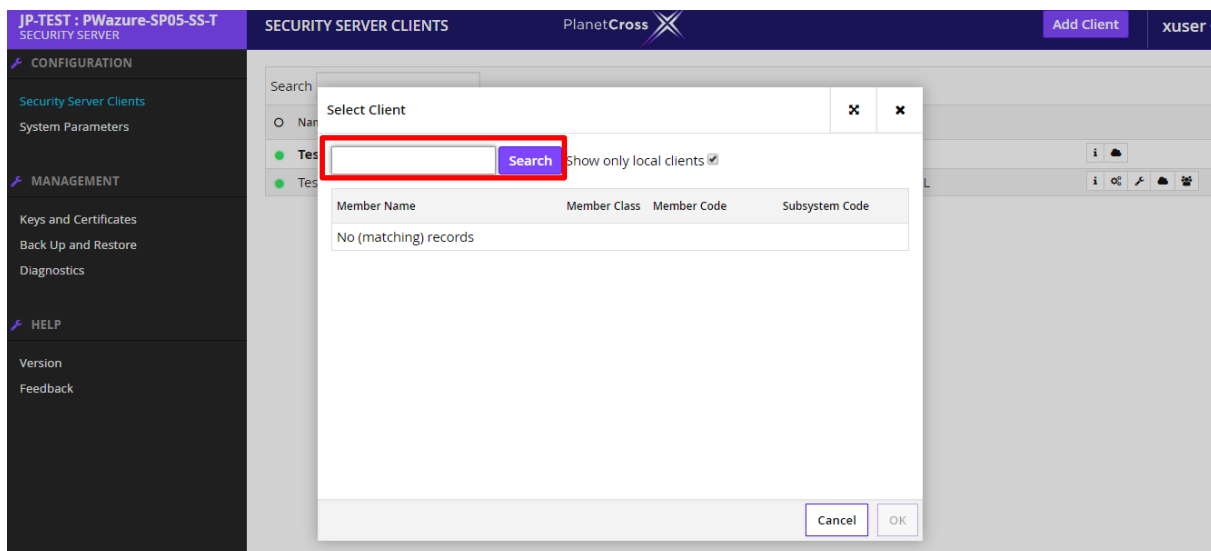
Add a timestamp service to the security server: <Access rights: **Registration Officer**>

1. On the **[Configuration]** menu, select **[Security Server Clients]**.



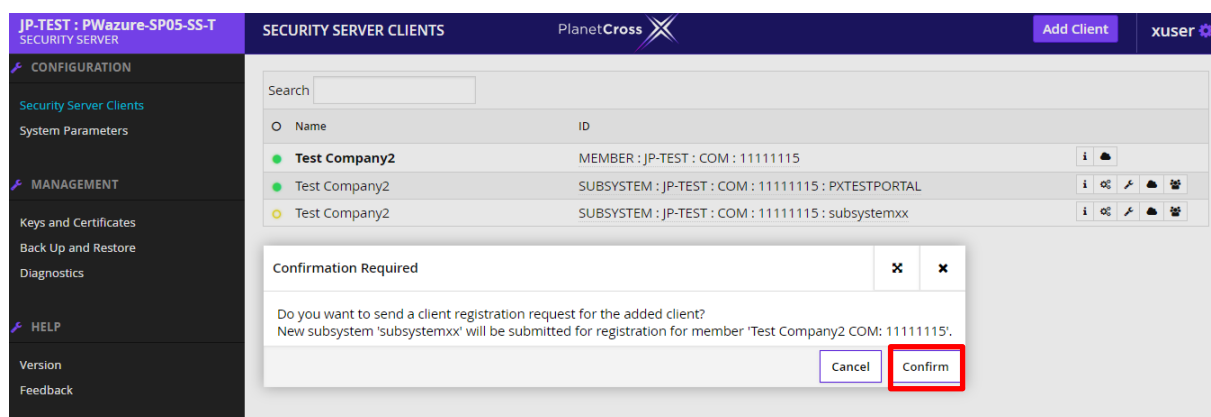
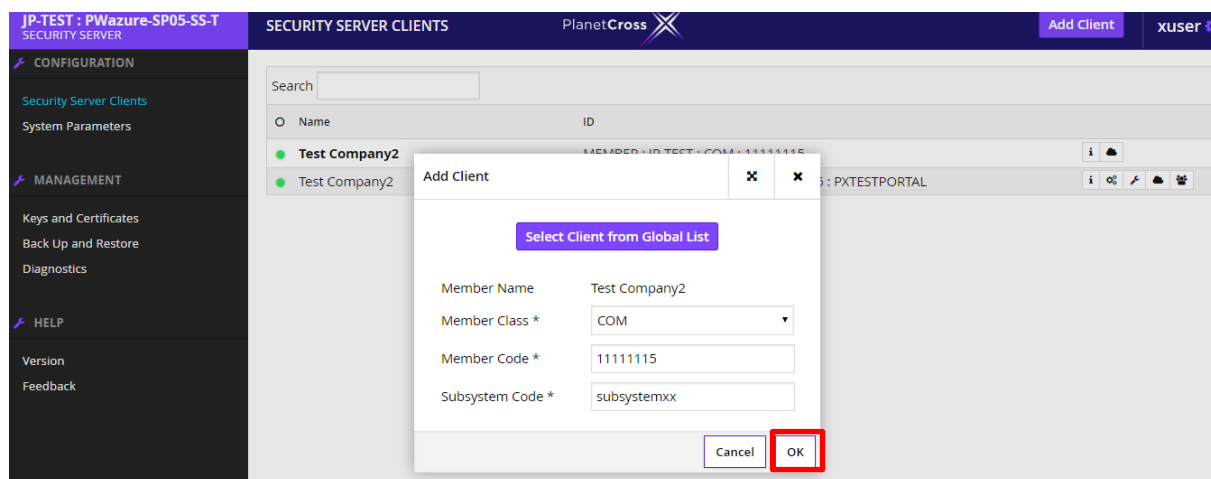
2. Click **[Add Client]**
In the window that opens, either enter the client's information manually or click **[Select Client from Global List]** and locate the client's information from within all PlanetCross members and their subsystems. Enter the client's information manually.





3. Click **[OK]** and **[Confirm]**

The new client is added to the list of security server clients in the "Saved" state.



3.3 Configuring a Signing Key and Certificate for a Security Server Client

A signing key and certificate must be configured for the security server client to sign messages exchanged over the PlanetCross.

【Note】

- Certificates are not issued to subsystems; therefore, the certificate of the subsystem's owner (that is, an PlanetCross member) is used for the subsystem.
- All particular PlanetCross member's subsystems that are registered in the same security server use the same signing certificate for signing messages. Hence, if the security server already contains the member's signing certificate, it is not necessary to configure a new signing key and/or certificate when adding a subsystem of that member.

3.4 Registering a Security Server Client in the PlanetCross Governing Authority

To register a security server client in the PlanetCross governing authority, the following actions must be completed.

1. The security server client registration request must be submitted from the security server.
2. A request for registering the client must be submitted to the PlanetCross governing authority according to the organizational procedures of the PlanetCross instance.

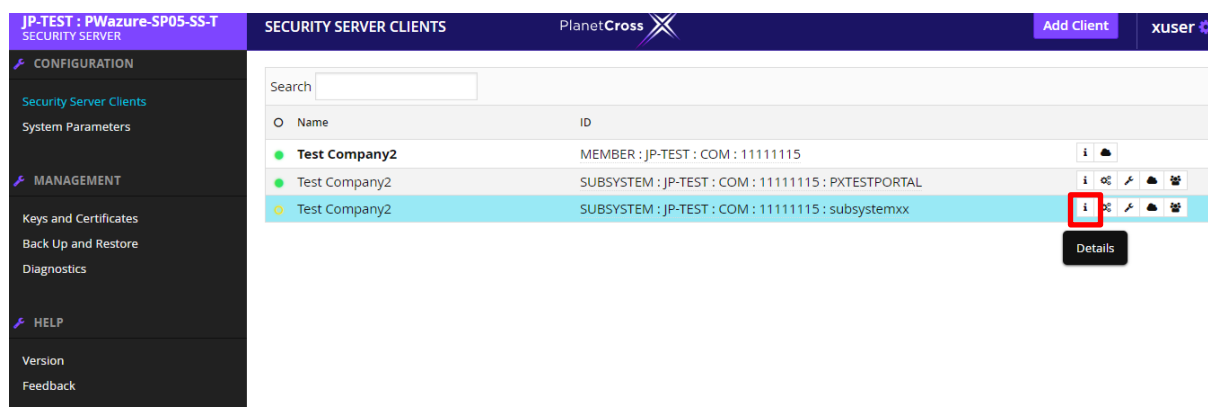
The registration request must be approved by the PlanetCross governing authority.

3.4.1 Registering a Security Server Client

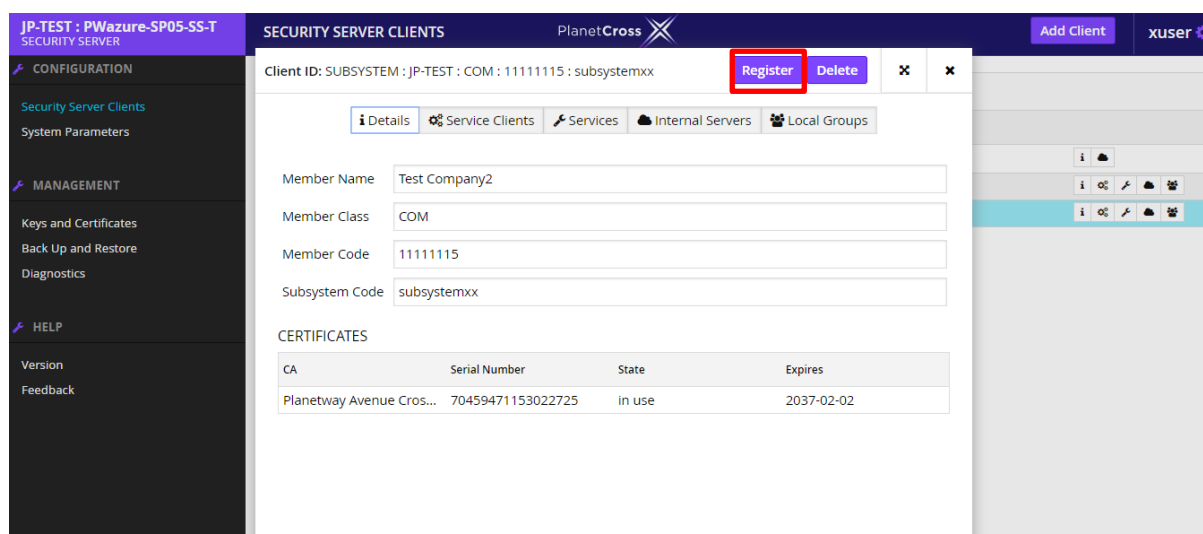
To submit a client registration request follow these steps.

<Access rights: **Registration Officer**>

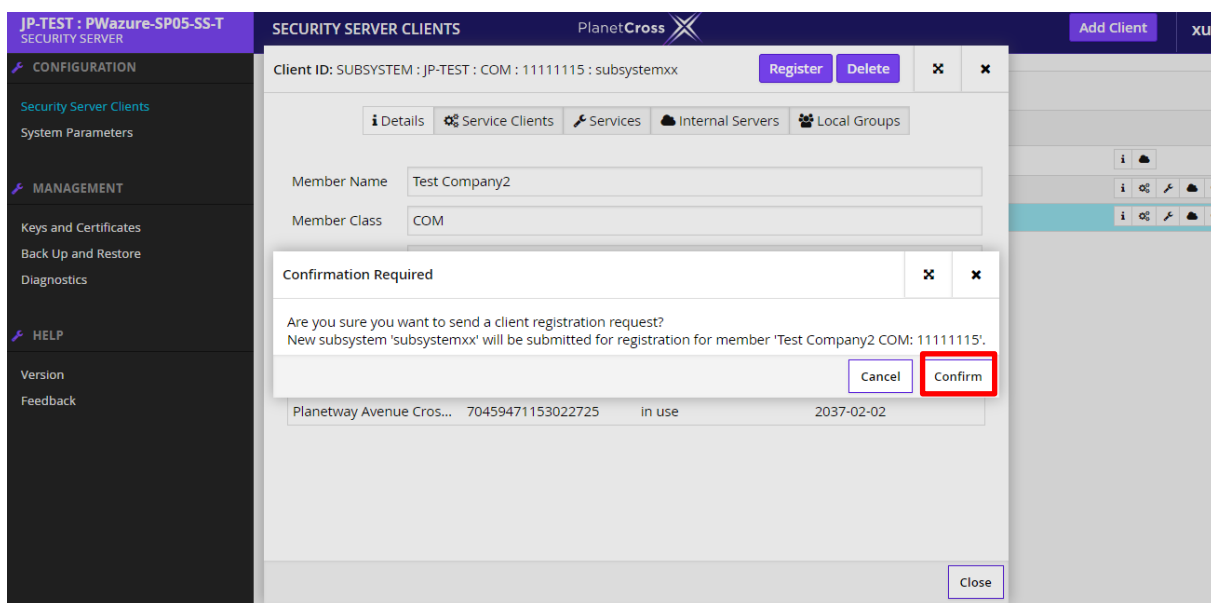
1. On the **[Configuration]** menu, select **[Security Server Clients]**
2. Select the client in the "Saved" state from the list of security server clients.



3. Click the **[Details]** icon and in the window that opens, click **[Register]**.



4. Click the **[Confirm]** to submit the request.



On submitting the request, the message "Request sent" is displayed, and the client's state is set to "Registration in process". After the PlanetCross governing authority has accepted the registration, the state of the client is set to "Registered" and the registration process is completed.

Check the Security Server Clients and make sure that State has changed from Yellow to Green.

3.5 Deleting a Client from the Security Server

If a client is deleted from the security server, all the information related to the client is deleted from the server as well – that is, the WSDLs, services, access rights, and, if necessary, the certificates.

【Note】

When one of the clients is deleted, it is not advisable to delete the signing certificate if the certificate is used by other clients registered to the security server, e.g., other subsystems belonging the same PlanetCross member as the deleted subsystem.

A client registered or submitted for registration in the PlanetCross governing authority (indicated by the "Registered" or "Registration in progress" state) must be unregistered before it can be deleted. The unregistering event sends a security server client deletion request from the security server to the central server.

3.5.1 Unregistering a Client

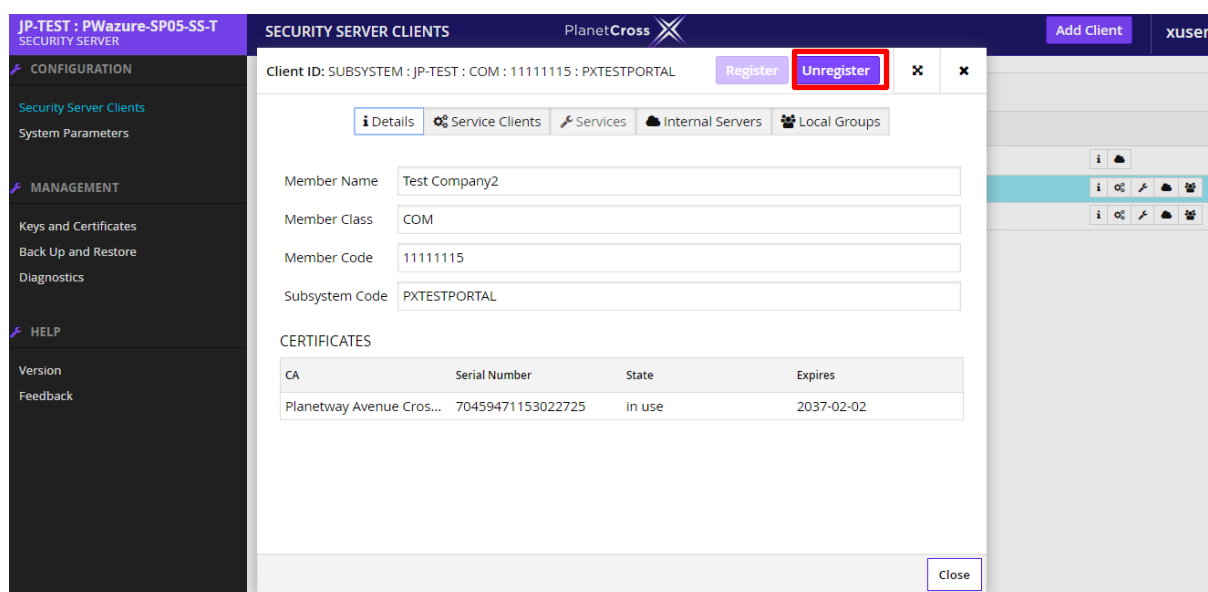
To unregister a client, follow these steps. <Access rights: **Registration Officer**>

1. On the **[Configuration]** menu, select **[Security Server Clients]**.
2. Select the client that you wish to remove from the server and click the **[Details]** icon on the client's row.

The screenshot shows the PlanetCross Security Server Clients management interface. The left sidebar contains a 'CONFIGURATION' menu with 'Security Server Clients' selected. The main area displays a table of clients. The second row, 'Test Company2' with ID 'SUBSYSTEM : JP-TEST : COM : 11111115 : PXTESTPORTAL', is highlighted. A red box highlights the 'Details' icon (an 'i' in a circle) in the action column of this row. A tooltip labeled 'Details' is visible below the icon.

Name	ID	Action
Test Company2	MEMBER : JP-TEST : COM : 11111115	[Icons]
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : PXTESTPORTAL	[Details] [Icons]
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : subsystemxx	[Icons]

3. In the window that opens, click **[Unregister]** and then click **[Confirm]**.



The security server automatically sends a client deletion request to the PlanetCross central server, upon the receipt of which the association between the security server and the client is revoked.

4. Next, a notification is displayed about sending a deletion request to the central server, and a confirmation is presented about deleting the client's information (except its certificates).

If you wish to delete the client's information immediately, click **[Confirm]**. Next, an option is presented to delete the client's certificates. To delete the certificates, click **[Confirm]** again.

If you wish to retain the client's information, click **[Cancel]**. In that case, the client is moved to the "Deletion in progress" state, wherein the client cannot mediate messages and cannot be registered again in the PlanetCross governing authority.

5. To delete the information of a client in the "Deletion in progress" state, select the client by clicking the **[Details]** icon on its row, click **[Delete]** in the window that opens, and then click **[Confirm]**.

【Note】

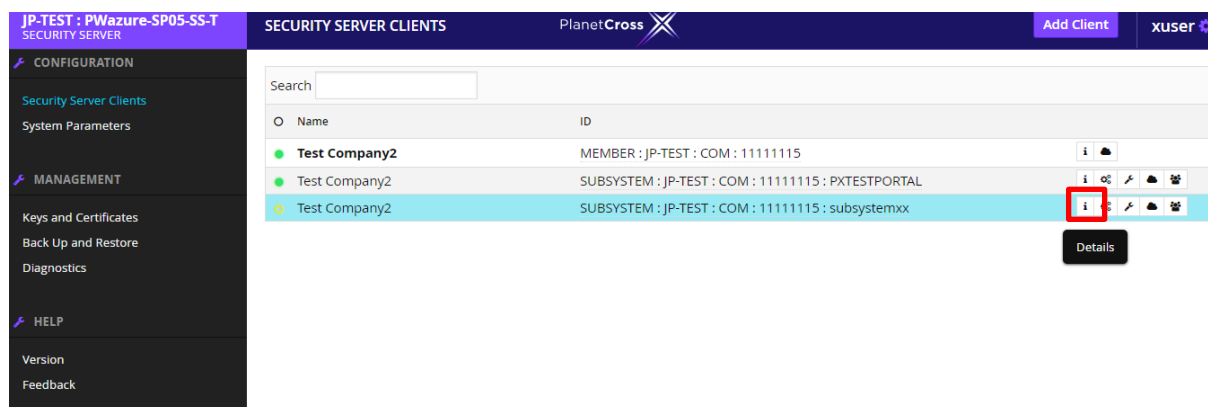
It is possible to unregister a registered client from the central server without sending a deletion request through the security server. In this case, the security server's administrator responsible for the client must transmit a request containing information about the client to be unregistered to the central server's administrator. If the client has been deleted from the central server without a prior deletion request from the security server, the client is shown in the "Global error" state in the security server.

3.5.2 Deleting a Client

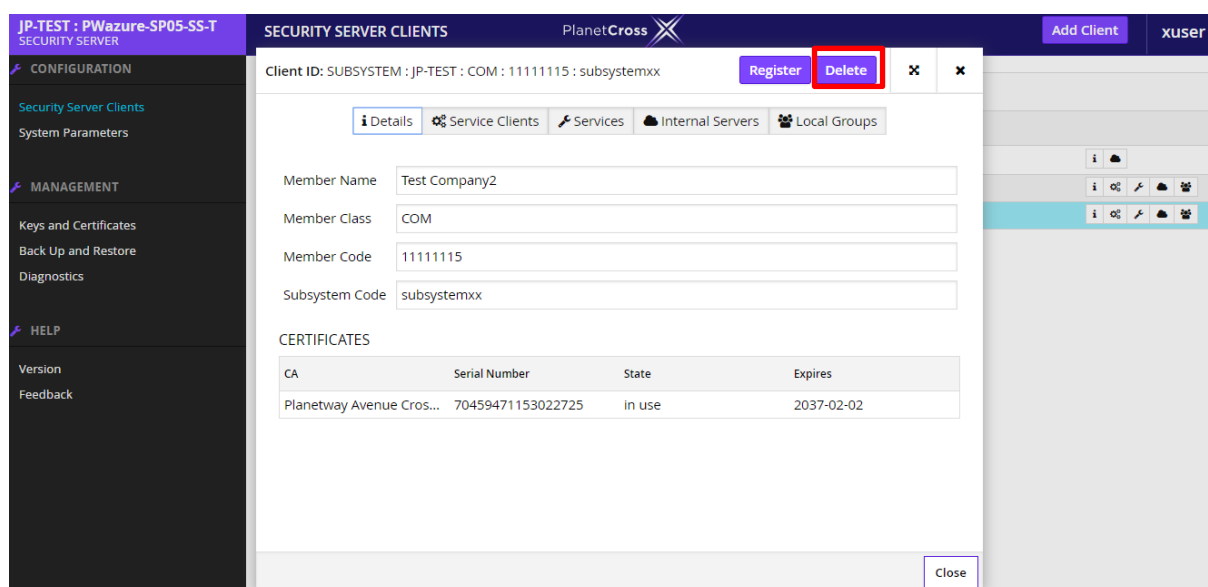
A security server client can be deleted if its state is "Saved", "Global error" or "Deletion in progress". Clients that are in states "Registered" or "Registration in progress" need to be unregistered before they can be deleted.

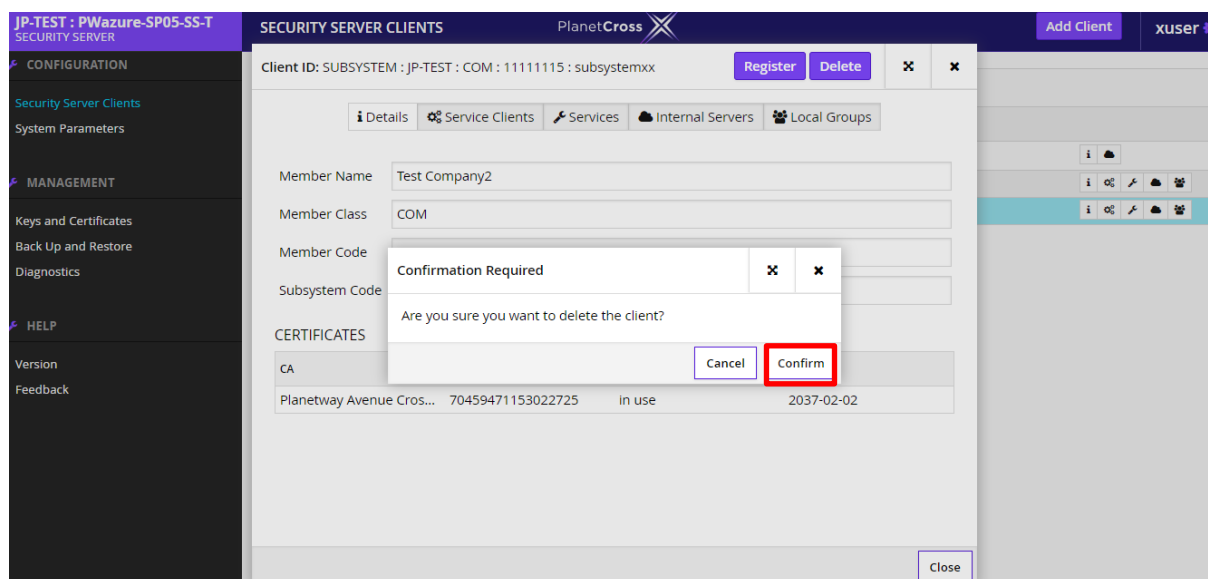
To delete a client, follow these steps. <Access rights: **Registration Officer**>

1. On the **[Configuration]** menu, select **[Security Server Clients]**.
2. Select from the table a client that you wish to remove from the security server and click the **[Details]** icon on that row.



3. In the window that opens, click **[Delete]**.



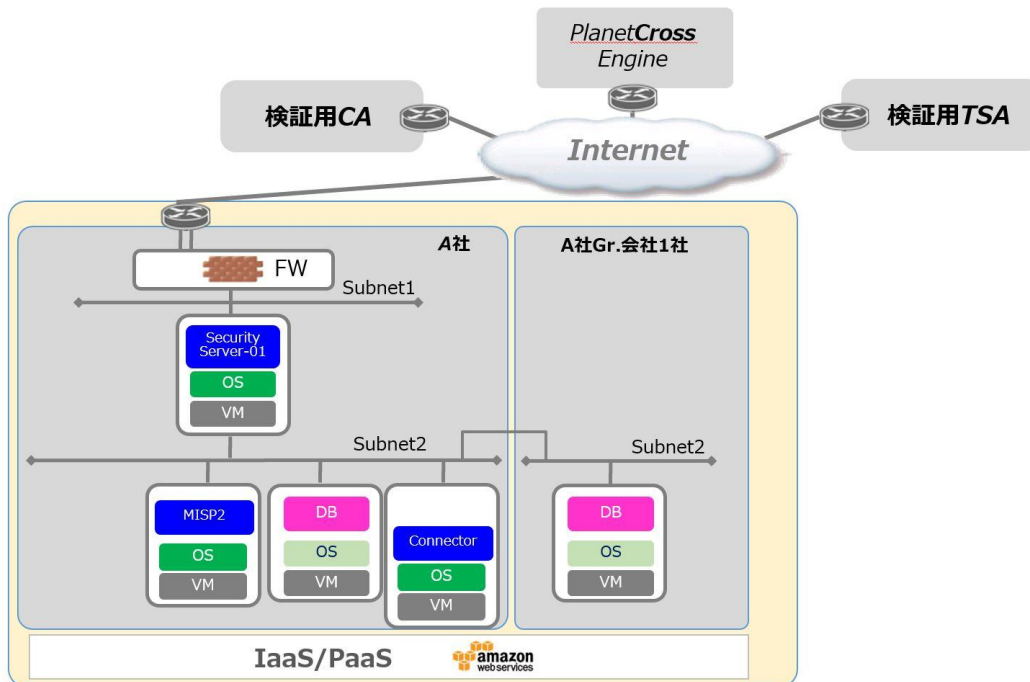
4. Confirm the deletion by clicking **[Confirm]**.

3.6 Registering multiple members to Security Server

Describe how to register multiple members to Security Server.

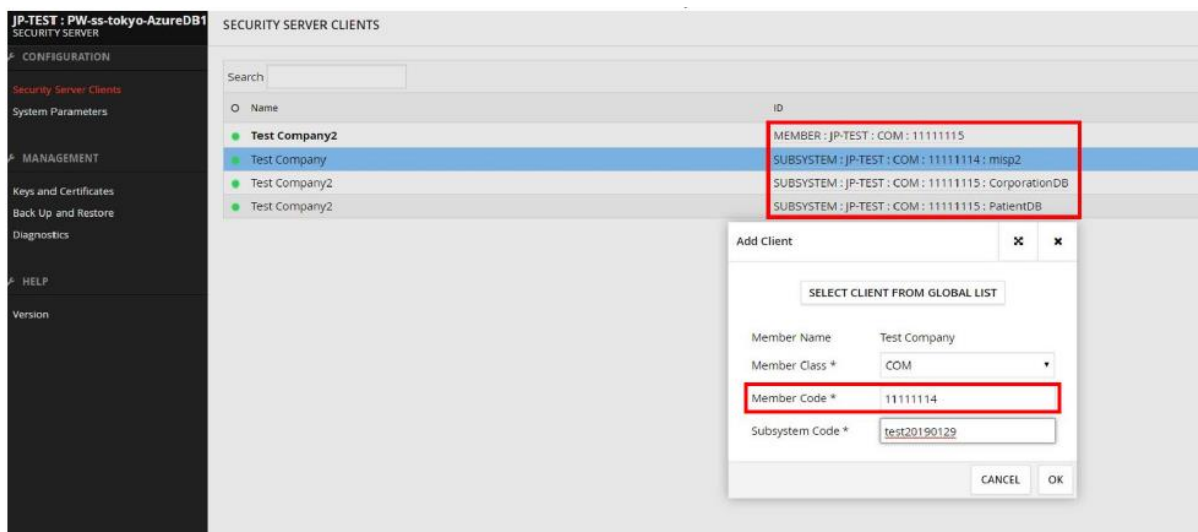
3.6.1 In case use one security server with multiple organization

Following case, A company and Group company A are using one security server on AWS.



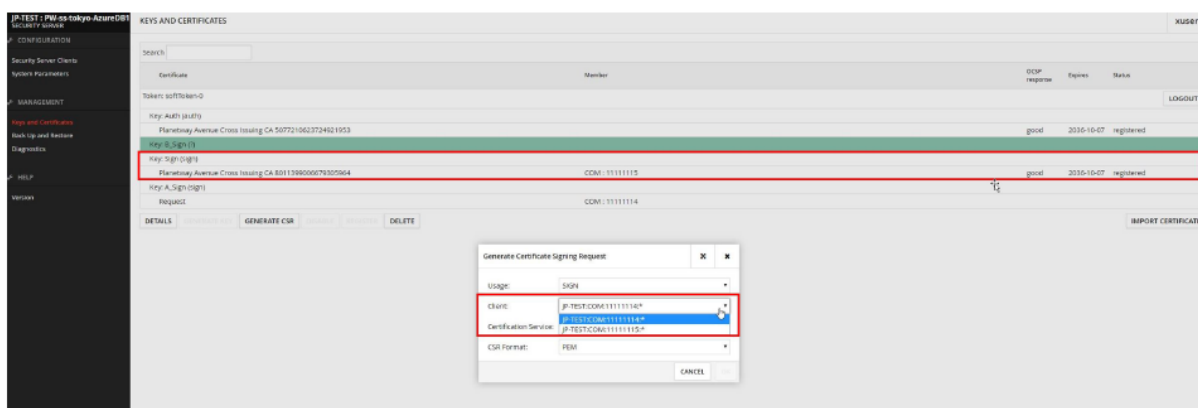
1. Register Member Code multiple times.
Ask Planetway Japan staff to register the Member Code.
2. Create Subsystem Client with multiple organization Member Codes.
 - (1) Click [Security Server Clients] > [Add client].

- (2) Create Subsystem Client with Member Code which is different from Security Server's Member Code.



3. Import certificate files multiple times.

- (1) Create Sign key clicking [Keys and Certificates].
- (2) Create CSR clicking [Generate CSR].



- (3) Import certificates files created from CSR. And the work is finished.

4. Security Tokens, Keys, and Certificates

4.1 Availability States of Security Tokens, Keys, and Certificates

To display the availability of objects (that is, tokens, keys or certificates), the following background colors are used in the "Keys and Certificates" view.

Background color	State
Yellow	The object is available to the security server, but the object's information has not been saved to the security server configuration. For example, a smartcard could be connected to the server, but the certificates on the smartcard may not have been imported to the server. Certificates on the yellow background cannot be used for mediating messages.
White	The object is available to the security server and the object's information has been saved to the security server's configuration. Certificates on the white background can be used for mediating messages.
Gray	The object is not available for the security server. Certificates on the gray background cannot be used for mediating messages.

【Note】


The key device's and key's information is automatically saved to the configuration when a certificate associated with either of them is imported to the security server, or when a certificate signing request is generated for the key. Similarly, the key device's and key's information is deleted from the security server configuration automatically upon the deletion of the last associated certificate and/or certificate signing request.

4.2 Registration States of Certificates

Registration states indicate if and how a certificate can be used in the PlanetCross system. In the "Keys and Certificates" view, a certificate's registration states (except "Deleted") are displayed in the "Status" column.






4.2.1 Registration States of the Signing Certificate

A security server signing certificate can be in one of the following registration states.

Status	Explanation
 Registered	The certificate has been imported to the security server and saved to its configuration. A signing certificate in a "Registered" state can be used for signing PlanetCross messages.
Deleted	The certificate has been deleted from the server configuration. If the certificate is in the "Deleted" state and stored on a hardware key device connected to the security server, the certificate is displayed on a yellow background.

4.2.2 Registration States of the Authentication Certificate

A security server authentication certificate can be in one of the following registration states.

Status	Explanation
 Saved	<p>The certificate has been imported to the security server and saved to its configuration, but the certificate has not been submitted for registration. From this state, the certificate can move to the following states:</p> <ul style="list-style-type: none"> • "Registration in progress" : if the authentication certificate registration request is sent from the security server to the central server; • "Deleted" : if the authentication certificate's information is deleted from the security server configuration.
 Registration in progress	<p>An authentication certificate registration request has been created and sent to the central server, but the association between the certificate and the security server has not yet been approved. From this state, the certificate can move to the following states:</p> <ul style="list-style-type: none"> • "Registered" : if the association between the authentication certificate and the security server is approved by the PlanetCross governing authority; • "Deletion in progress" : if the certificate deletion request has been submitted to the central server. The user can force this state transition even if the sending of the authentication certificate deletion request fails.
 Registered	<p>The association between the authentication certificate and the security server has been approved in the central server. An authentication certificate in this state can be used to establish a secure data exchange channel for exchanging PlanetCross messages. From this state, the certificate can move to the following states:</p> <ul style="list-style-type: none"> • "Global error" : if the association between the authentication certificate and the security server has been revoked in the central server; • "Deletion in progress" : if the certificate deletion request has been transmitted to the central server. The user can force this state transition even if the sending of the authentication certificate deletion request fails.
 Global error	<p>The association between the authentication certificate and the security server has been revoked in the central server. From this state, the certificate can move to the following states:</p> <ul style="list-style-type: none"> • "Registered" : if the association between the authentication certificate and the security server has been restored in the central server (e.g., the association between the client and the security server was lost due to an error); • "Deleted" : if the authentication certificate's information is deleted from the security server configuration.
 Deletion in progress	<p>An authentication certificate deletion request has been created for the certificate and sent to the central server. From this state, the certificate can move to the following state:</p> <ul style="list-style-type: none"> • "Deleted" : if the authentication certificate's information is deleted from the security server configuration.
Delete	The certificate has been deleted from the security server configuration.

4.3 Validity States of Certificates

Validity states indicate if and how a certificate can be used independent of the PlanetCross system. In the "Keys and Certificates" view, the certificate's validity states are displayed in the "OCSP response" column. Validity states (except "Disabled") are displayed for certificates that are in the "Registered" registration state.

A security server certificate can be in one of the following validity states.

Validity states	Explanation
Unknown (validity information missing)	The certificate does not have a valid OCSP response (the OCSP response validity period is set by the PlanetCross governing authority) or the last OCSP response was either "unknown" (the responder doesn't know about the certificate being requested) or an error.
Suspended	The last OCSP response about the certificate was "suspended".
Good (valid)	The last OCSP response about the certificate was "good". Only certificates in the "good" (valid) state can be used to sign messages or establish a connection between security servers.
Expired	The certificate's validity end date has passed. The certificate is not active and OCSP queries are not performed about it.
Revoked	The last OCSP response about the certificate was "revoked". The certificate is not active and OCSP queries are not performed about it.
Disabled	the user has marked the certificate as disabled. The certificate is not active and OCSP queries are not performed about it.

4.4 Activating and Disabling the Certificates

Disabled certificates are not used for signing messages or for establishing secure channels between security servers (authentication). If a certificate is disabled, its status in the “OCSP response” column in the “Keys and Certificates” table is “Disabled”.

To activate or disable a certificate, follow these steps.

<Access rights : For authentication certificates: Security Officer>

<Access rights : For signing certificates: Security Officer , Registration Officer>

1. On the **[Management]** menu, select **[Keys and Certificates]**.
2. To activate a certificate, select an inactive certificate from the table and click **[Activate]**.

Search

Certificate	Member	OCSP response	Expires	Status
Token: softToken-0				
Key: Authkey (auth)				
Planetway Avenue Cross Issuing CA 745025238153862808		disabled	2037-02-03	saved
Key: Signkey (sign)				
Planetway Avenue Cross Issuing CA 38472...	COM : 11111115	good	2037-02-03	registered

Details

Generate Key

Generate CSR

Activate

Register

Delete

Import certificate

To deactivate a certificate, select an active certificate from the table and click **[Disable]**.

JP-TEST : PWazure-SP05-SS-T
SECURITY SERVER

CONFIGURATION

Security Server Clients

System Parameters

MANAGEMENT

Keys and Certificates

Back Up and Restore

Diagnostics

HELP

Version

Feedback

KEYS AND CERTIFICATES

PlanetCross

xuser

Search

Certificate	Member	OCSP response	Expires	Status
Token: softToken-0				
Key: Sign Key (sign)				
Planetway Avenue Cross Issuing CA 70459471153022725	COM : 11111115	good	2037-02-02	registered
Key: Auth Key (auth)				
Planetway Avenue Cross Issuing CA 774...		good	2037-02-02	registered

Details

Generate Key

Generate CSR

Disable

Register

Delete

Import certificate

4.5 Configuring and Registering an Authentication key and Certificate

A Security server can have multiple authentication keys and certificates (e.g., during authentication key change).

The following is described in 『Security Server Installation Guide』

- The process of configuring another authentication key and certificate
- The process of registering an authentication certificate

4.6 Deleting a Certificate

An authentication certificate registered or submitted for registration in the PlanetCross governing authority (indicated by the "Registered" or "Registration in progress" state) must be unregistered before it can be deleted. The unregistering event sends an authentication certificate deletion request from the security server to the central server.

4.6.1 Unregistering an Authentication Certificate

To unregister an authentication certificate, follow these steps.

<Access rights: **Security Officer**>

1. On the **[Management]** menu, select **[Keys and Certificates]**.
2. Select an authentication certificate in the state "Registered" or "Registration in progress" and click **[Unregister]**.

The screenshot shows the PlanetCross Security Server interface. The left sidebar contains a menu with 'CONFIGURATION' (Security Server Clients, System Parameters), 'MANAGEMENT' (Keys and Certificates, Back Up and Restore, Diagnostics), and 'HELP' (Version, Feedback). The main area is titled 'KEYS AND CERTIFICATES' and features a search bar, a table of certificates, and a row of action buttons. The 'Unregister' button is highlighted with a red box.

Certificate	Member	OCSP response	Expires	Status
Token: softToken-0				
Key: Sign Key (sign)				
Planetway Avenue Cross Issuing CA 704...	COM : 111111115	good	2037-02-02	registered
Key: Auth Key (auth)				
Planetway Avenue Cross Issuing CA 7740353447306764211		good	2037-02-02	registered

Buttons: Details, Generate Key, Generate CSR, Disable, **Unregister**, Delete, Import certificate

Next, an authentication certificate deletion request is automatically sent to the PlanetCross central server, upon the receipt of which the associated authentication certificate is deleted from the central server. If the request was successfully sent, the message "Request sent" is displayed and the authentication certificate is moved to the "Deletion in progress" state.

【Note】

A registered authentication certificate can be deleted from the central server without sending a deletion request through the security server. In this case, the security server's administrator must transmit a request containing information about the authentication certificate to be deleted to the central server's administrator. If the authentication certificate has been deleted from the central server without a deletion request from the security server, the certificate is shown in the "Global

error" state in the security server.

4.6.2 Deleting a Certificate or a certificate Signing Request notice

An authentication certificate saved in the system configuration can be deleted if its state is "Saved", "Global error" or "Deletion in progress". The signing certificate and request notices can always be deleted from the system configuration.

If a certificate is stored on a hardware security token, then the deletion works on two levels:

- if the certificate is saved in the server configuration, then the deletion deletes the certificate from server configuration, but not from the security token;
- if the certificate is not saved in the server configuration (the background of the certificate is yellow), then the deletion deletes the certificate from the security token (assuming the token supports this operation).

To delete a certificate or a signing request(CSR) notice, follow these steps.

<Access rights : For authentication certificates: **Security Officer**>

<Access rights : For signing certificates: **Security Officer , Registration Officer**>

1. On the **[Management]** menu, select **[Keys and Certificates]**.
2. Select from the table a certificate or a certificate signing request(CSR) notice and click **[Delete]**.

The screenshot shows the PlanetCross Security Server interface. The top header includes the title 'JP-TEST : PWazure-SP05-SS-T SECURITY SERVER', the 'KEYS AND CERTIFICATES' section title, the PlanetCross logo, and a user profile 'xuser'. The left sidebar has a 'MANAGEMENT' section with 'Keys and Certificates' selected. The main content area shows a table of certificates. The table has columns for 'Certificate', 'Member', 'OCSP response', 'Expires', and 'Status'. One certificate is highlighted in blue, and the 'Delete' button is highlighted with a red box.

Certificate	Member	OCSP response	Expires	Status
Token: softToken-0				
Key: Sign Key (sign)				
Planetway Avenue Cross Issuing CA 70459471153022725	COM : 11111115	good	2037-02-02	registered
Key: Auth Key (auth)				
Planetway Avenue Cross Issuing CA 774...		good	2037-02-02	registered

Buttons: Details, Generate Key, Generate CSR, Disable, Register, **Delete**, Import certificate

3. Confirm the deletion by clicking **[Confirm]**.

4.7 Deleting a Key

Warning

Deleting a key from the server configuration also deletes all certificates (and certificate signing request(CSR) notices) associated with the key.

The deletion of keys works on two levels:

- If the key is saved in the server configuration, then the deletion deletes the key (and associated certificates) from server configuration, but not from the security token;
- If the key is not saved in the server configuration (the background of the key is yellow), then the deletion deletes the key from the security token (assuming the token supports this operation).

To delete a key, follow these steps.

<Access rights : For authentication keys: **Security Officer**>

<Access rights : For signing keys: **Security Officer , Registration Officer**>

<Access rights : For keys without a role: **Security Officer , Registration Officer**>

1. On the **[Management]** menu, select **[Keys and Certificates]**.
2. Select a key and click **[Delete]**.

The screenshot shows the PlanetCross Security Server interface. The top header includes the system name 'JP-TEST : PWazure-SP05-SS-T', the title 'KEYS AND CERTIFICATES', the PlanetCross logo, and the user 'xuser'. The left sidebar has a 'MANAGEMENT' section with 'Keys and Certificates' selected. The main content area has a search bar and a table with columns: Certificate, Member, OCSP response, Expires, and Status. There are two rows of keys. Below the table, there are buttons: Details, Generate Key, Generate CSR, Disable, Register, and Delete (highlighted with a red box). An 'Import certificate' button is also present.

Certificate	Member	OCSP response	Expires	Status
Token: softToken-0				
Logout				
Key: Sign Key (sign)				
Planetway Avenue Cross Issuing CA 704...	COM : 11111115	good	2037-02-02	registered
Key: Auth Key (auth)				
Planetway Avenue Cross Issuing CA 774...		good	2037-02-02	registered

Buttons: Details, Generate Key, Generate CSR, Disable, Register, Delete, Import certificate

3. Confirm the deletion of the key (and its associated certificates) by clicking **[Confirm]**.

5. Setting a Service

5.1 PlanetCross Service

The services are managed on two levels:

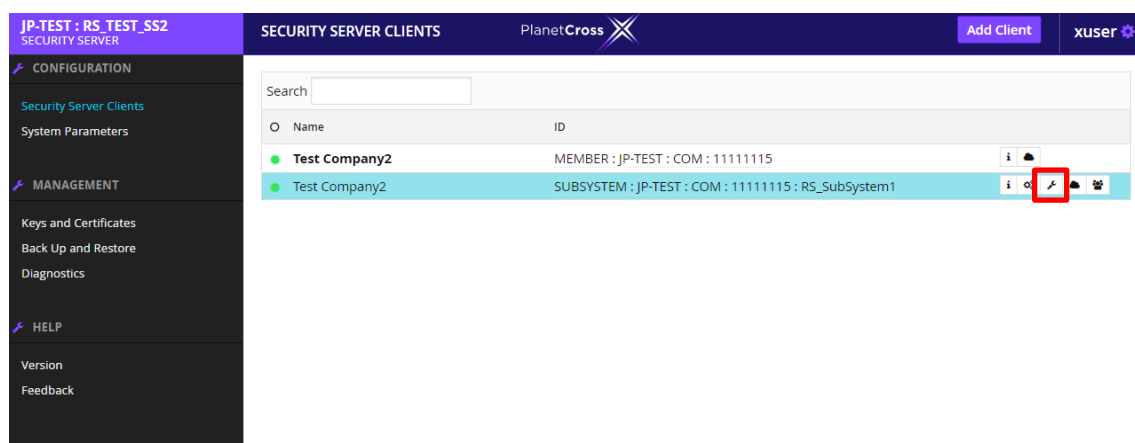
- The addition, deletion, and deactivation of services is carried out on the WSDL level;
- The service address, internal network connection method, and the service timeout values are configured at the service level. However, it is easy to extend the configuration of one service to all the other services in the same WSDL.

5.2 Adding a WSDL

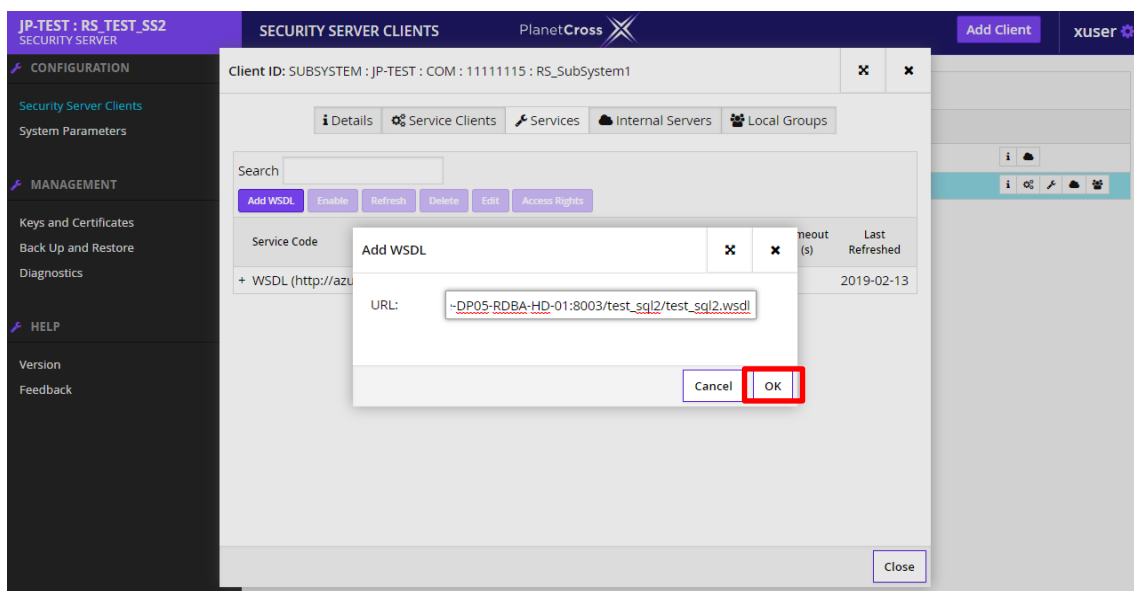
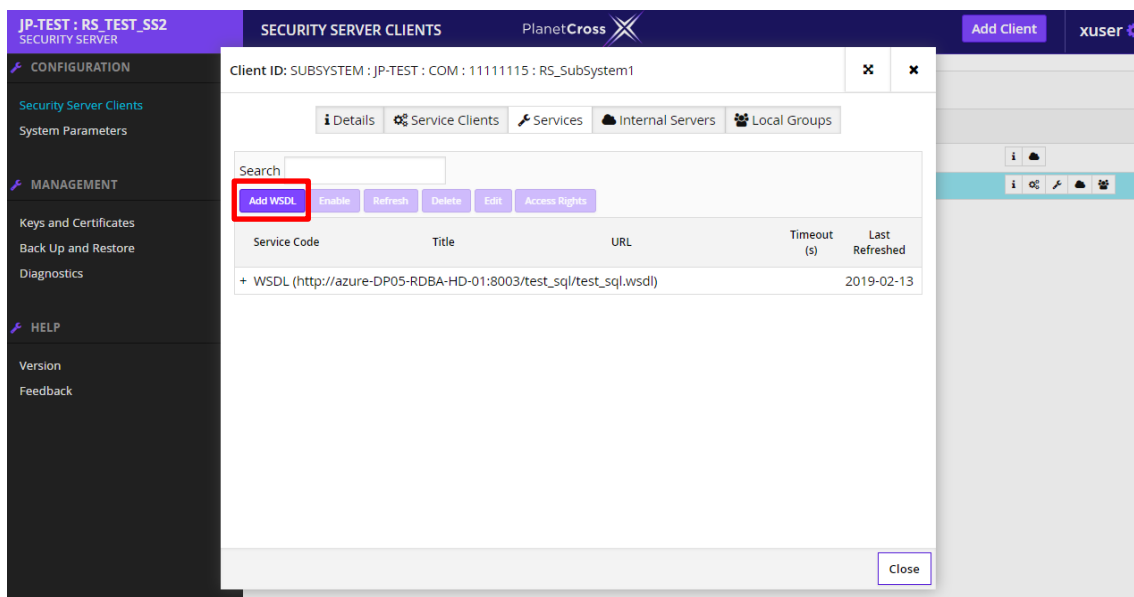
When a new WSDL file is added, the security server reads service information from it and displays the information in the table of services. The service code, title and address are read from the WSDL.

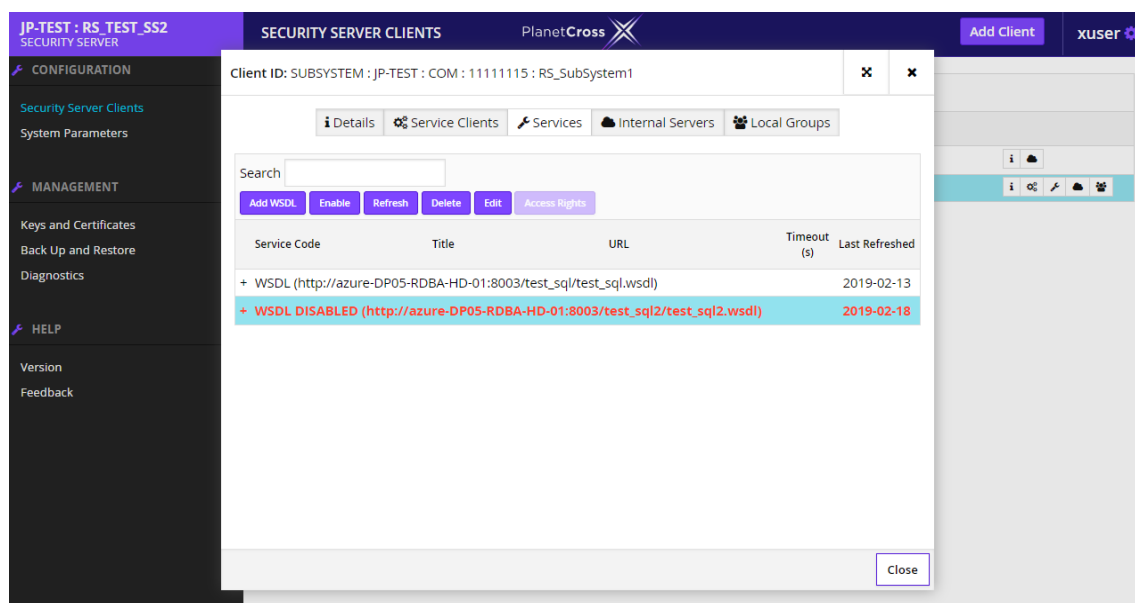
To add a WSDL, follow these steps. <Access rights: **Service Administrator**>

1. On the **[Configuration]** menu, select **[Security Server Clients]**, select a client from the table and click the **[Services]** icon on that row.



2. Click **[Add WSDL]**, enter the WSDL address in the window that opens and click **[OK]**. The WSDL and the information about the services it contains are added to the table. By default, the WSDL is added in disabled state.





To see a list of services contained in the WSDL.

- Click the “+” symbol in front of the WSDL row to expand the list.

5.3 Refreshing a WSDL

Upon refreshing, the security server reloads the WSDL file from the WSDL address to the security server and checks the service information in the reloaded file against existing services. If the composition of services in the new WSDL has changed compared to the current version, a warning is displayed and you can either continue with the refresh or cancel.

To refresh the WSDL, follow these steps.

<Access rights: **Service Administrator**>

- On the **[Configuration]** menu, select **[Security Server Clients]**, select a client from the table and click the **[Services]** icon on that row.
- Select from the table a WSDL to be refreshed and click **[Refresh]**.
If the new WSDL contains changes compared to the current WSDL in the security server, a warning is displayed.
- If a warning is displayed, to proceed with the refresh, click **[Continue]**.

When the WSDL is refreshed, the existing services' settings are not overwritten.

5.4 Enabling and Disabling a WSDL

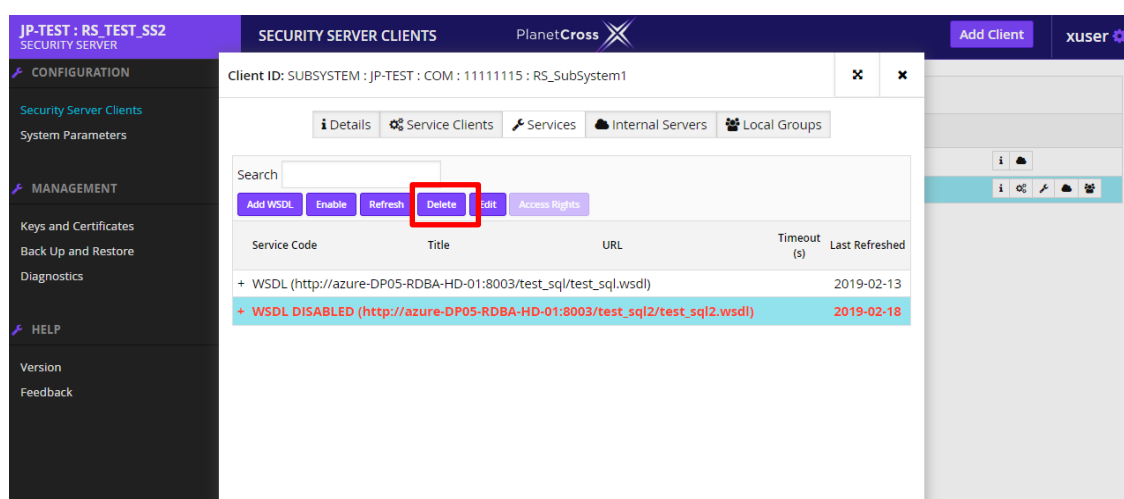
A disabled WSDL is displayed in the services' table in red with a "Disabled" note.

Services described by a disabled WSDL cannot be accessed by the service clients – if an attempt is made to access the service, an error message is returned, containing the information entered by the security server's administrator when the WSDL was disabled.

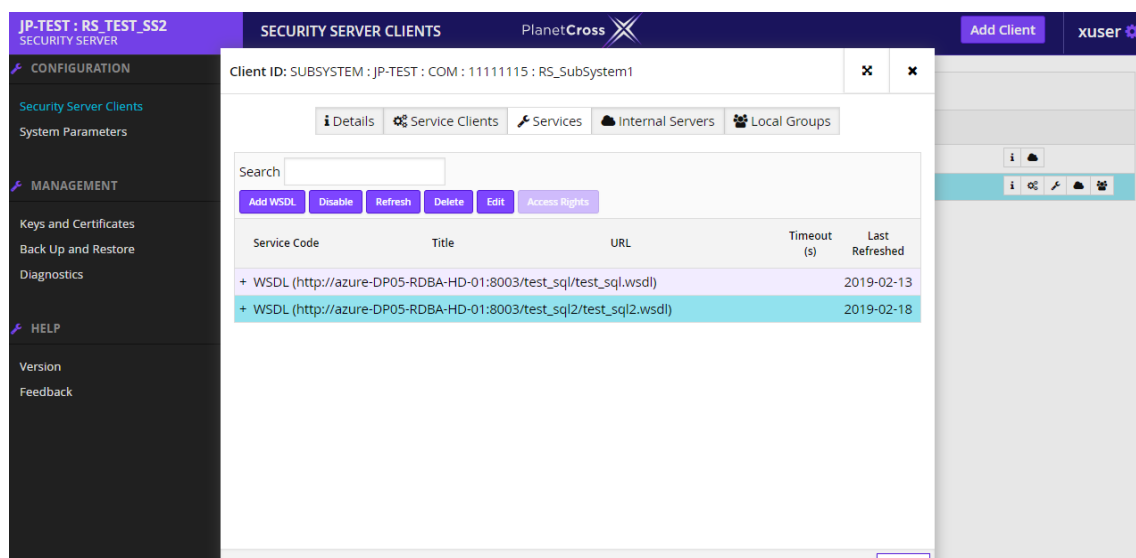
If a WSDL is enabled, the services described there become accessible to users. Therefore it is necessary to ensure that before enabling the WSDL, the parameters of all its services are correctly configured.

To enable a WSDL, follow these steps. <Access rights: **Service Administrator**>

1. On the **[Configuration]** menu, select **[Security Server Clients]**, select a client from the table and click the **[Services]** icon on that row.
2. Select a disabled WSDL from the table and click **[Enable]**.



After clicking, it becomes black and becomes valid.



To disable a WSDL, follow these steps.

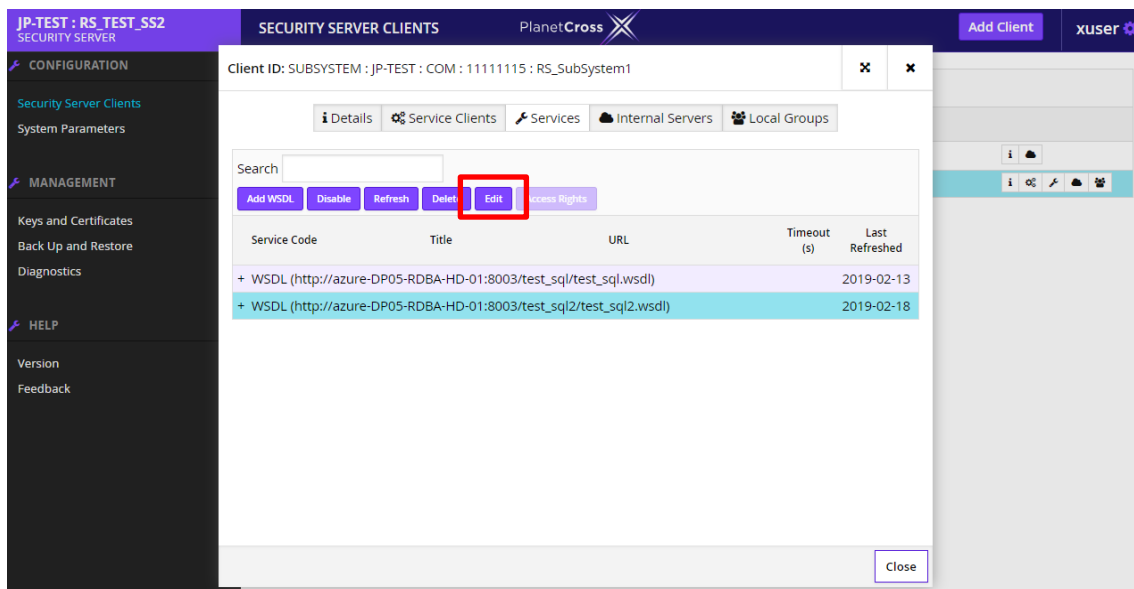
1. On the **[Configuration]** menu, select **[Security Server Clients]**, select a client from the table and click the **[Services]** icon on that row.
2. To disable a WSDL, select an enabled WSDL from the table and click **[Disable]**.
3. In the window that opens, enter an error message , which is shown to clients who try to access any of the services in the WSDL.
4. Finally click **[OK]**.

5.5 Changing the Address of a WSDL

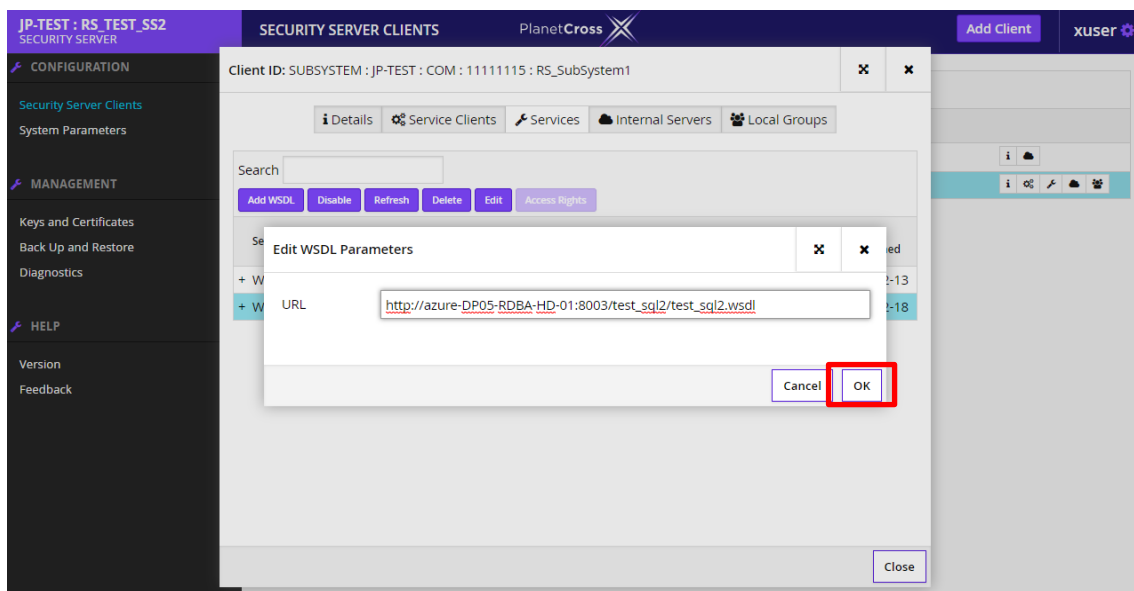
To change the WSDL address, follow these steps.WSDL

<Access rights: **Service Administrator**>

1. On the **[Configuration]** menu, select **[Security Server Clients]**, select a client from the table and click the **[Services]** icon on that row.
2. Select from the table a WSDL whose address you wish to change and click **[Edit]**.



3. In the window that opens, edit the WSDL address and click **[OK]**. When the address is changed, the WSDL is refreshed.



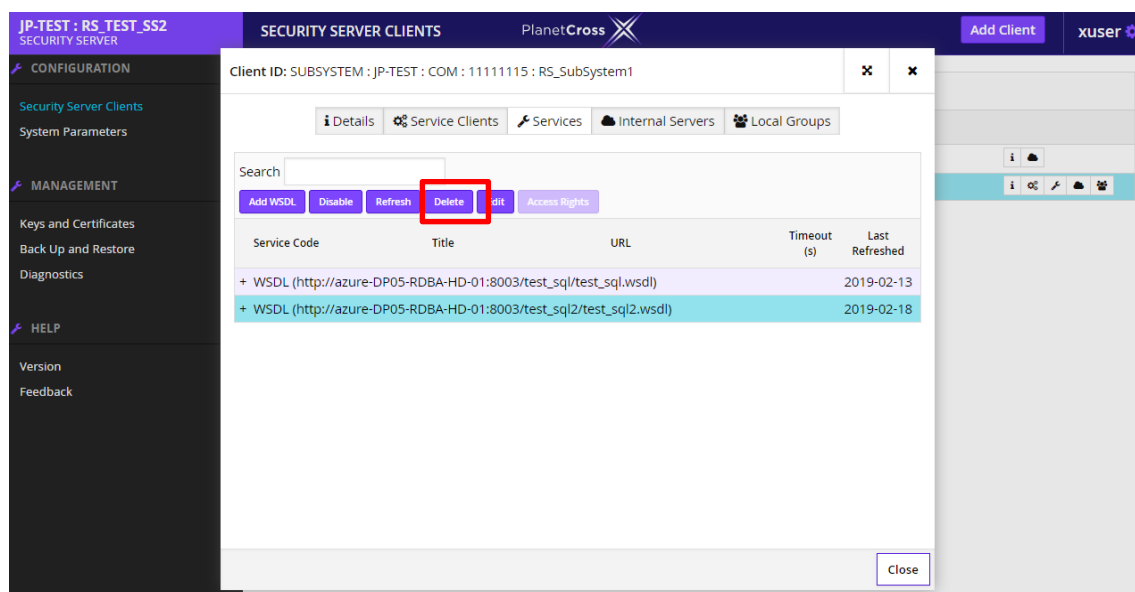
5.6 Deleting a WSDL

When a WSDL is deleted, all information related to the services described in the WSDL, including access rights, are deleted.

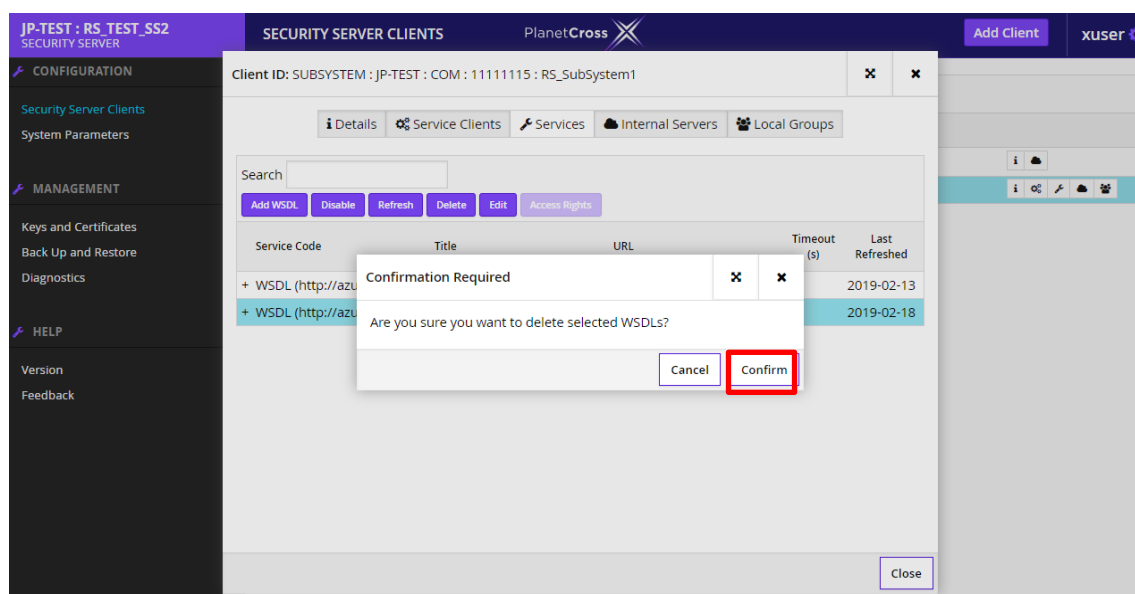
To delete a WSDL, follow these steps.

<Access rights: **Service Administrator**>

1. On the **[Configuration]** menu, select **[Security Server Clients]**, select a client from the table and click the **[Services]** icon on that row.
2. Select from the table a WSDL to be deleted and click **[Delete]**.



3. Confirm the deletion by clicking **[Confirm]** in the window that opens.



5.7 Changing the Parameters of a Service

Service parameters are

- **"Service URL"** - the URL where requests targeted at the service are directed;
- **"Timeout (s)"** - the maximum duration of a request to the database, in seconds;
- **"Verify TLS certificate"** - toggles the verification of the certificate when a TLS connection is established.

To change service parameters, follow these steps.

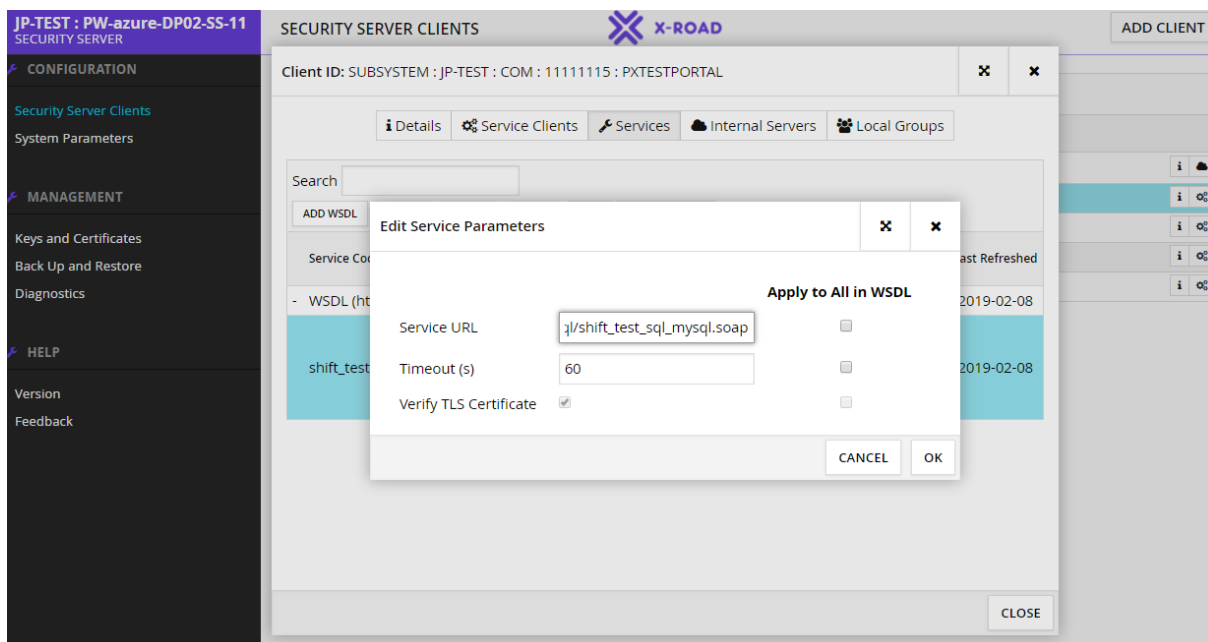
<Access rights: **Service Administrator**>

1. On the **[Configuration]** menu, select **[Security Server Clients]**, select a client from the table and click the **[Services]** icon on that row.
2. Select a service from the table and click **[Edit]**.

The screenshot shows the X-Road Security Server Clients interface. On the left is a sidebar with a menu including CONFIGURATION, MANAGEMENT, and HELP. The main area is titled 'SECURITY SERVER CLIENTS' and shows a modal window for a specific client. The modal has tabs for Details, Service Clients, Services, Internal Servers, and Local Groups. The 'Services' tab is active, displaying a table of services. The 'EDIT' button in the table's action column is highlighted with a red box. The table has columns for Service Code, Title, URL, Timeout (s), and Last Refreshed.

Service Code	Title	URL	Timeout (s)	Last Refreshed
- WSDL (http://azure-DP02-RDBA-03:8003/shift_test_sql_mysql/shift_test_sql_mysql.w...				2019-02-08
shift_test_sql_mysql.v1 (1)	Teenus shift_test_sql_mysql	http://azure-DP02-RDBA-03:8003/shift_test_sql_mysql/shift_test_sql_mysql.soap	60	2019-02-08

3. In the window that opens, configure the service parameters. To apply the selected parameter to all services described in the same WSDL , select the checkbox adjacent to this parameter in the **[Apply to All in WSDL]** column.



4. To apply the configured parameters, click **[OK]**.

6. Access Rights

Access rights can be granted to the following access right subjects. アクセス権は、以下のアクセス権の対象に付与することができます。

- **A PlanetCross member's subsystem.**
- **A global access rights group** - Global groups are created in the PlanetCross governing authority. If a group is granted an access right, it extends to all group members.
- **A local access rights group** - To simplify access rights management, each client in the security server can create local access rights groups. If a group is granted an access right, it extends to all group members.

There are two options for managing access rights in a security server.

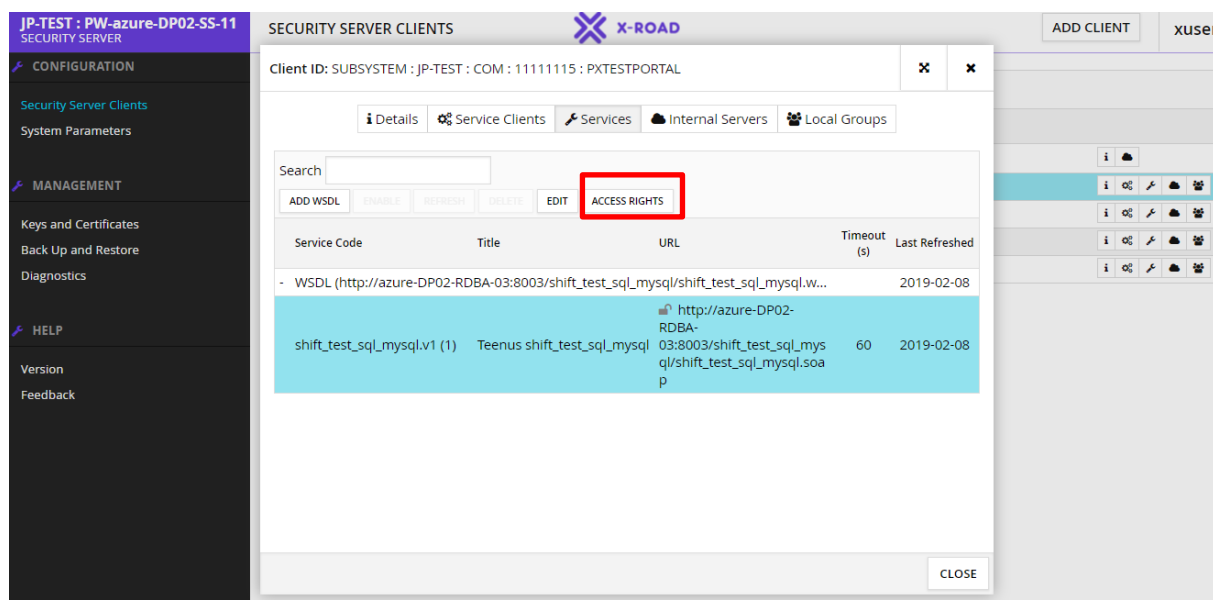
- **Service-based access rights management** - if a single service needs to be opened/closed to multiple service clients.
- **Service client-based access rights management** - if a single service client needs multiple services opened/closed.

6.1 Changing the Access Rights of a Service

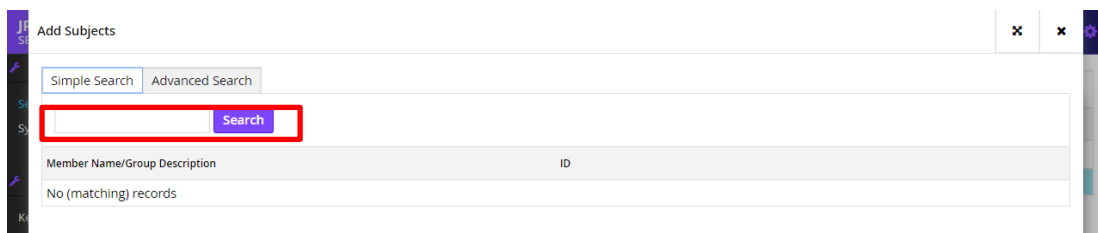
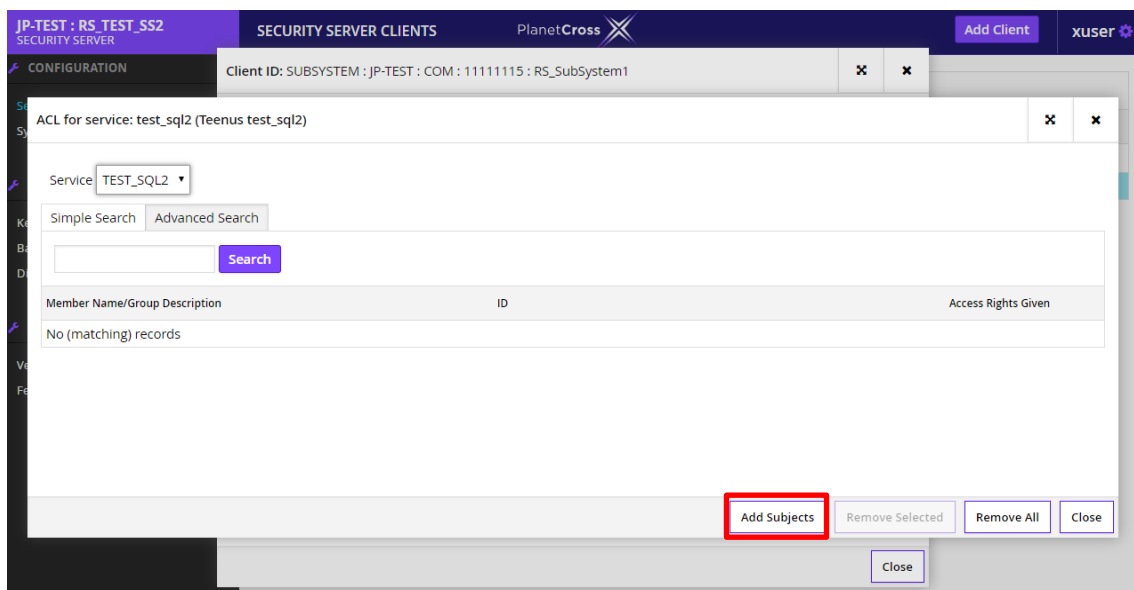
To change the access rights to a service, follow these steps.

<Access rights: **Service Administrator**>

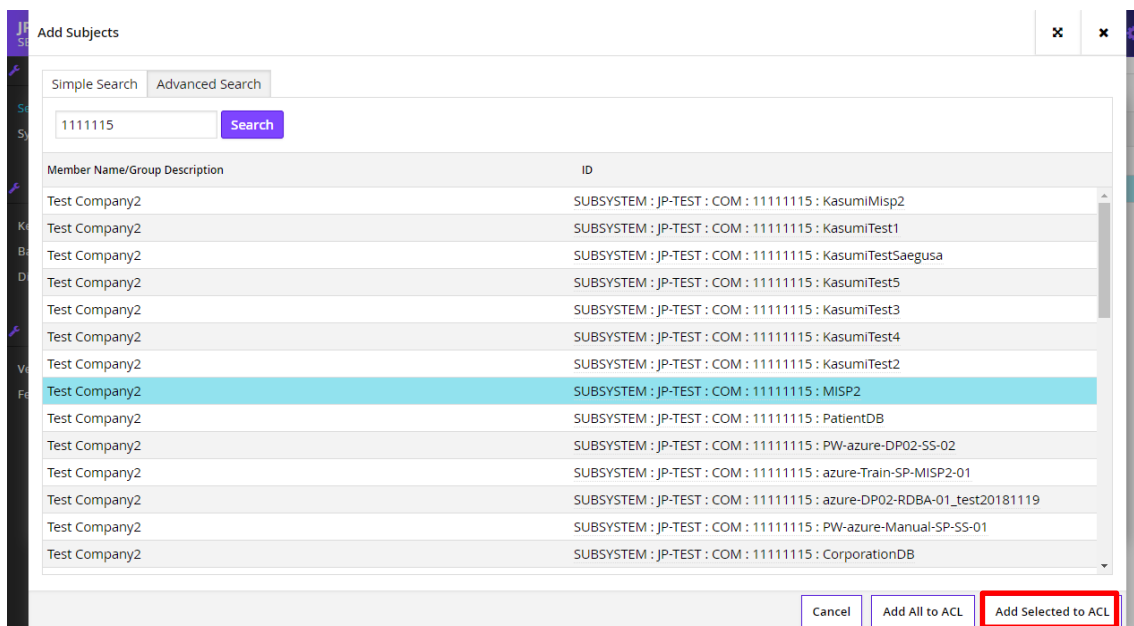
1. On the **[Configuration]** menu, select **[Security Server Clients]**, select a client from the table and click the **[Services]** icon on that row.
2. Select a service from the table and click **[Access Rights]**.
In the window that opens, the access rights table displays information about all PlanetCross subsystems and groups that have access to the selected service.



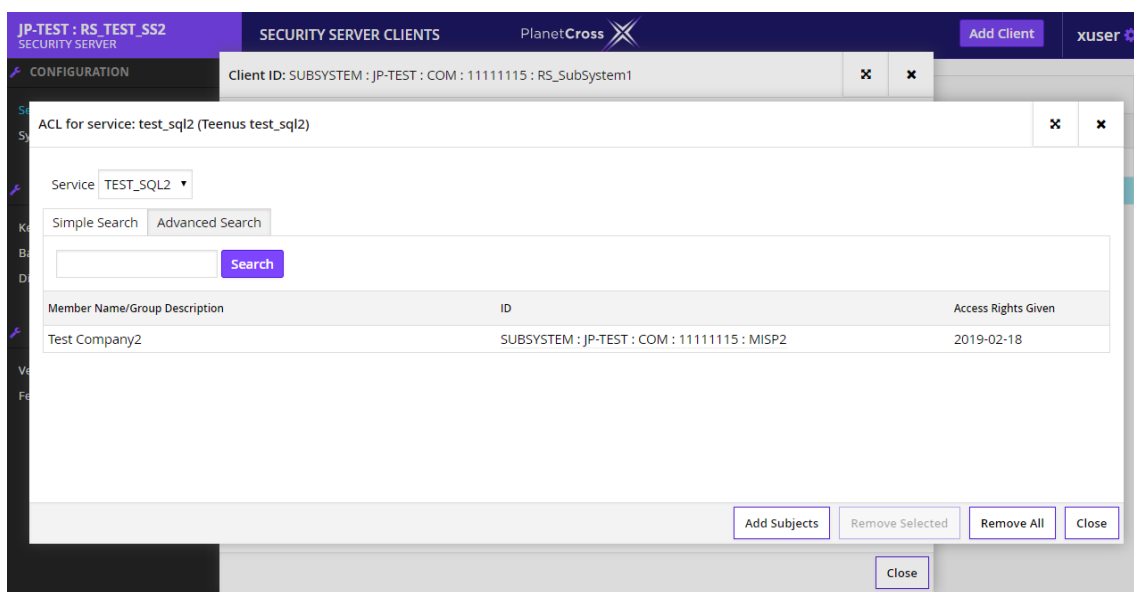
- To add one or more access right subjects to the service, click **[Add Subjects]**. The subject search window appears. You can search among all subsystems and global groups registered in the PlanetCross governing authority and among the security server client's local groups.



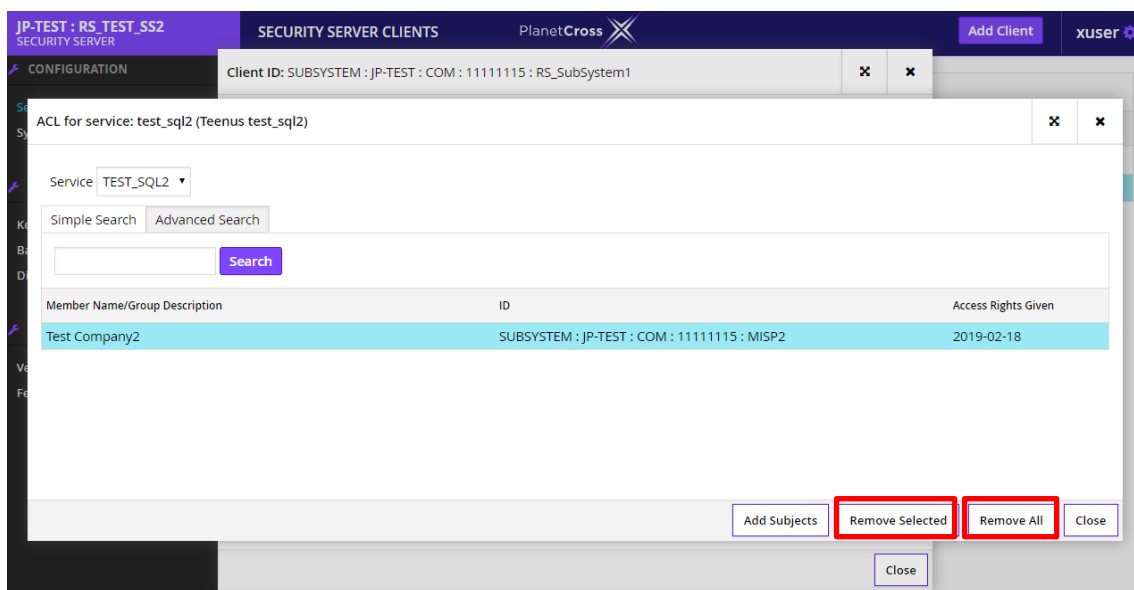
Select one or more subjects from the table and click **[Add Selected to ACL]**. To grant the access right to all subjects in the search results, click **[Add All to ACL]**.



After clicking, can see the subject with access rights.



4. To remove service access rights subjects, select the respective rows in the access rights table and click **[Remove Selected]**. To clear the access rights list (that is, remove all subjects), click **[Remove All]**.



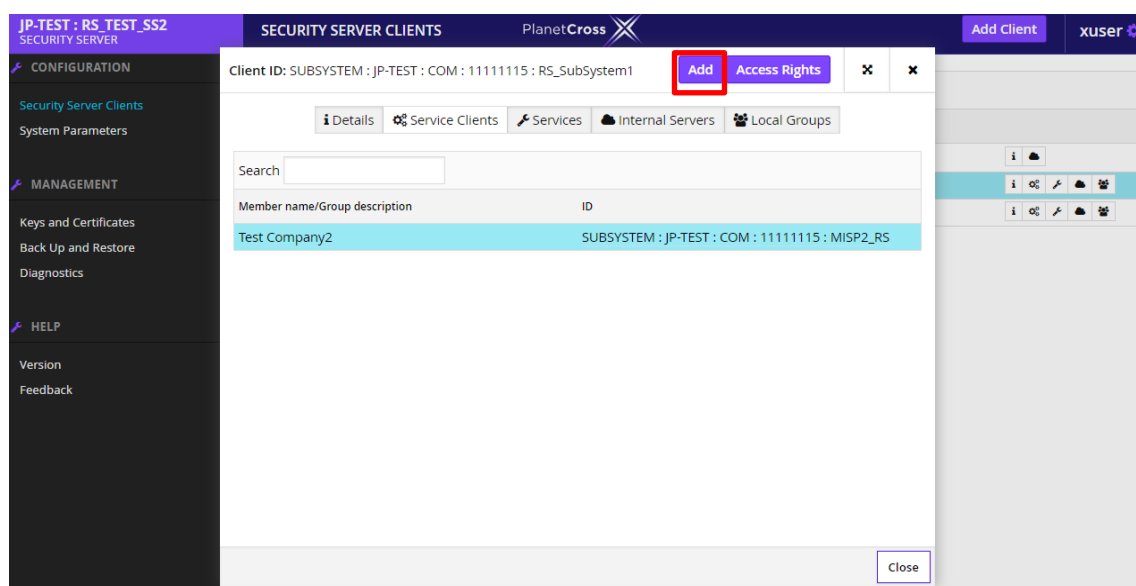
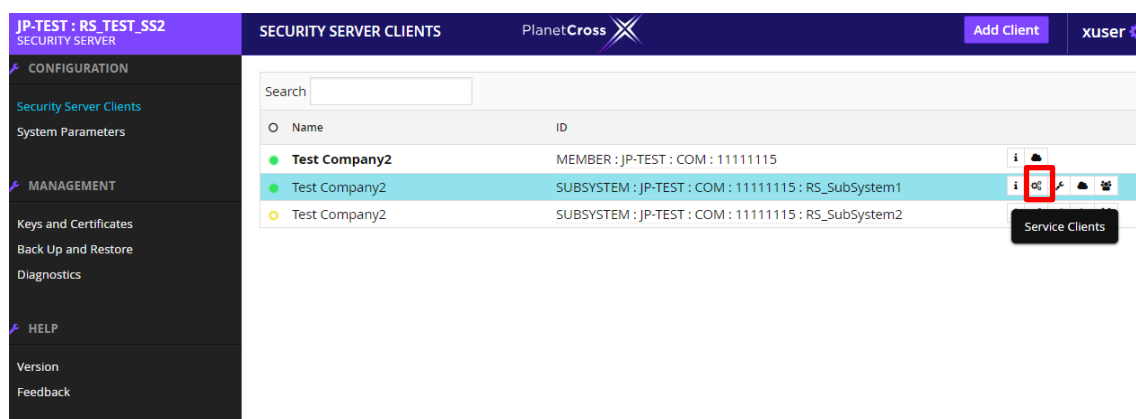
6.2 Adding a Service Client

The service client view (Configuration -> Security Server Clients -> Service Clients) displays all the access rights subjects of the services mediated by this security server client. In other words, if an PlanetCross subsystem or group has been granted the access right to a service of this client, then the subject is shown in this view.

To add a service client, follow these steps.

<Access rights: **Service Administrator**>

1. On the **[Configuration]** menu, select **[Security Server Clients]**.
2. Select a client from the table and click the **[Service Clients]** icon, then click **[Add]**.



3. In the window that opens, locate and select a subject (a subsystem, or a local or global group) to which you want to grant access rights to and click **[Next]**.

Add Subjects

Simple Search Advanced Search

Search

Member Name/Group Description	ID
No (matching) records	

Cancel Next

Add Subjects

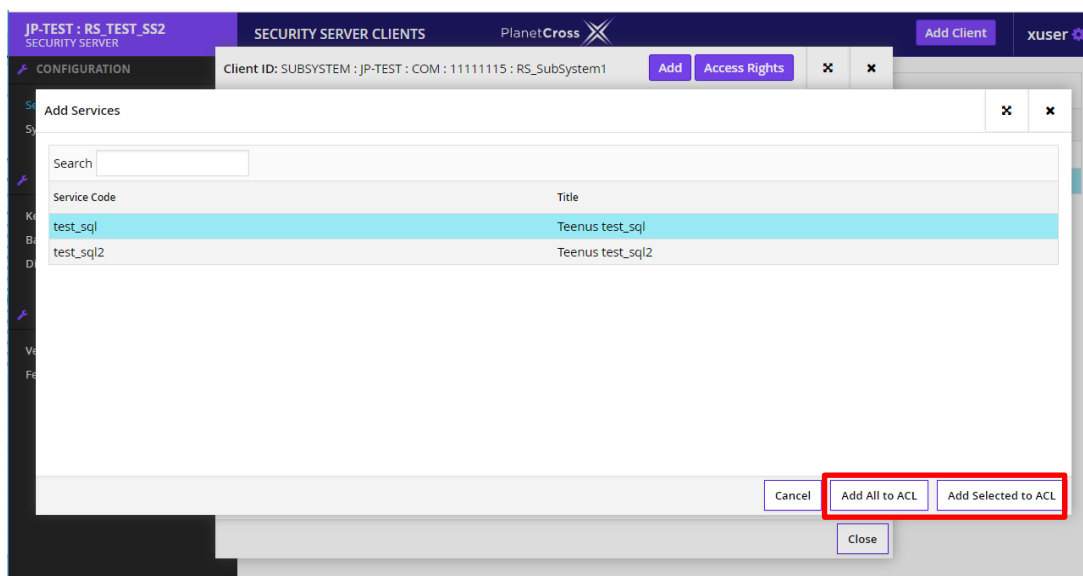
Simple Search Advanced Search

1111115 Search

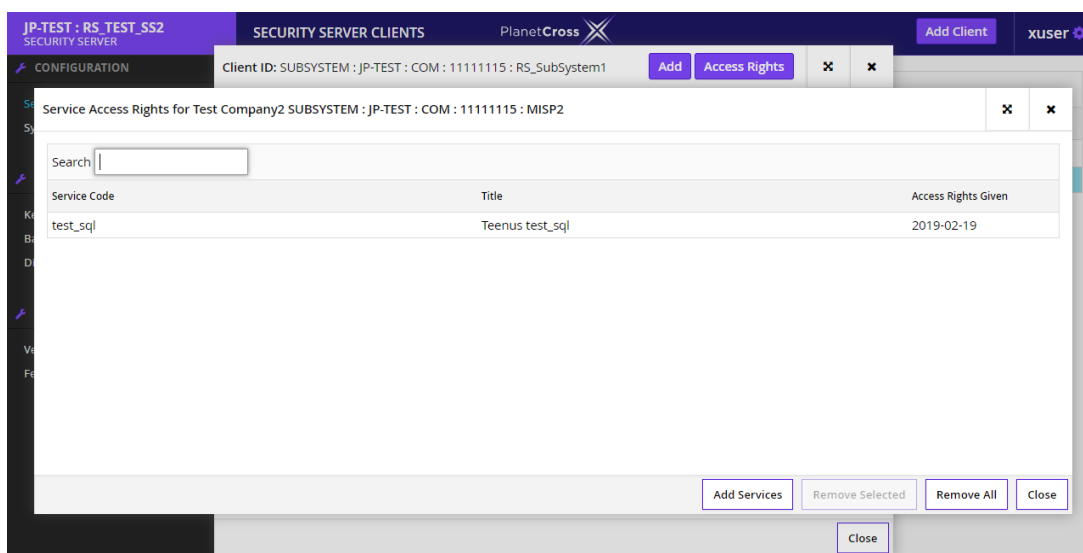
Member Name/Group Description	ID
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : KasumiMisp2
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : KasumiTest1
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : KasumiTestSaegusa
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : KasumiTest5
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : KasumiTest3
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : KasumiTest4
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : KasumiTest2
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : MISP2
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : PatientDB
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : PW-azure-DP02-SS-02
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : azure-Train-SP-MISP2-01
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : azure-DP02-RDBA-01_test20181119
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : PW-azure-Manual-SP-SS-01
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : CorporationDB

Cancel Next

4. Locate the service(s) whose access rights you want to grant to the selected subject.
5. Click **[Add Selected to ACL]** to grant access rights to the selected services to this subject.
Click **[Add All to ACL]** to grant access rights to all services in the filter to the subject.



The subject is added to the list of service clients, after which the service client's access rights view is displayed where the access rights can be changed.



6.3 Changing the Access Rights of a Service Client

To change the service client's access rights, follow these steps.

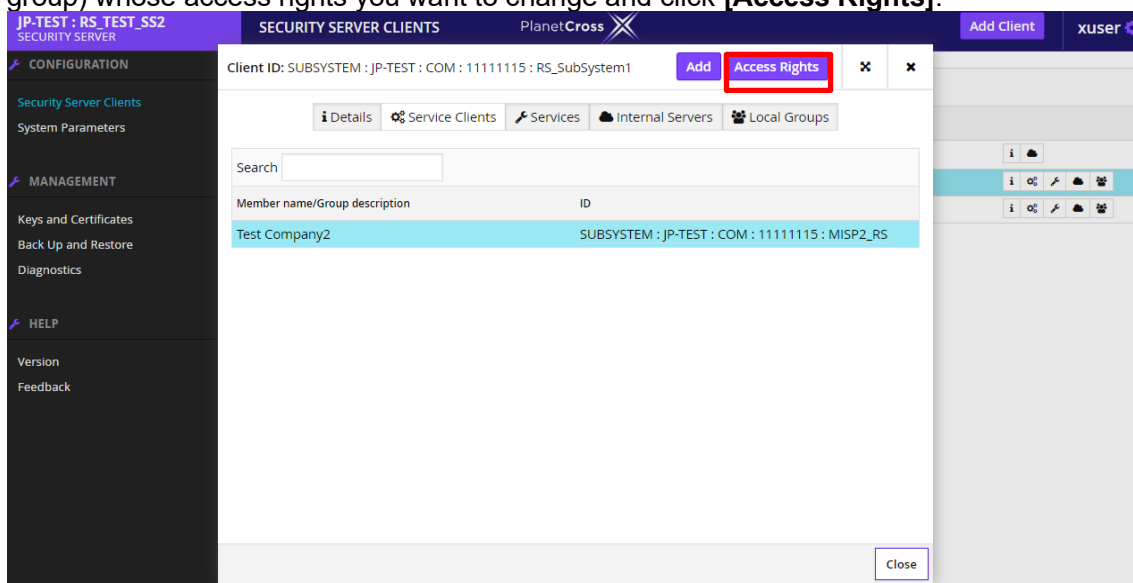
<Access rights: **Service Administrator**>

1. On the **[Configuration]** menu, select **[Security Server Clients]**, select a client from the table and click the **[Service Clients]** icon on that row.

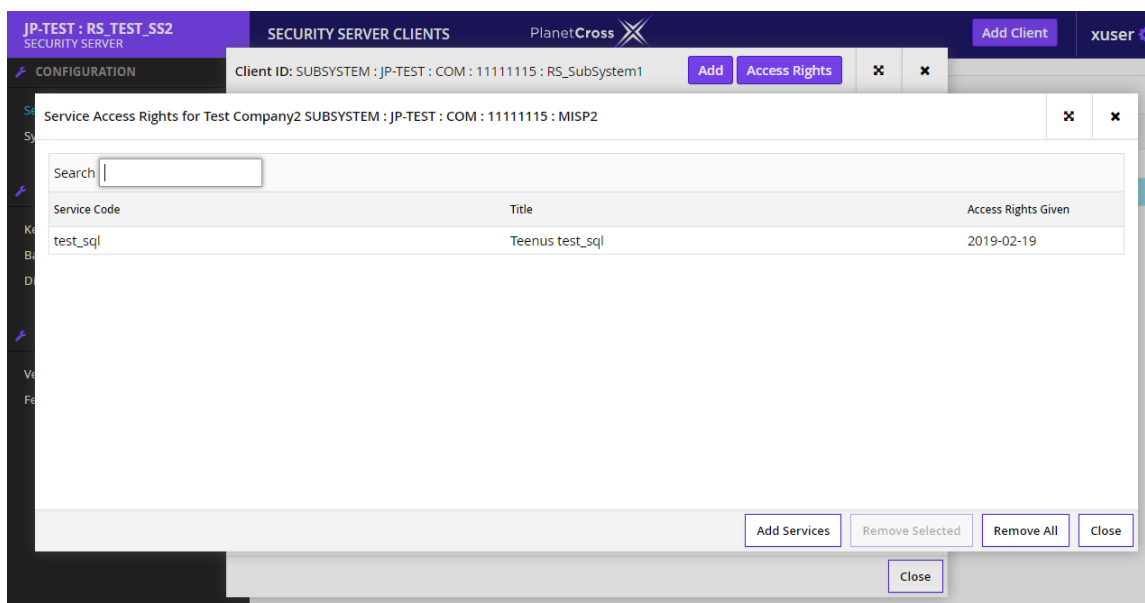
The screenshot shows the PlanetCross Security Server Clients management interface. The left sidebar contains a 'CONFIGURATION' menu with 'Security Server Clients' selected. The main area displays a table of clients. The second row, 'Test Company2' with ID 'SUBSYSTEM : JP-TEST : COM : 11111115 : RS_SubSystem1', is highlighted. A red box highlights the 'Service Clients' icon in the action column of this row.

Name	ID	Action
Test Company2	MEMBER : JP-TEST : COM : 11111115	[i] [lock] [plus]
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : RS_SubSystem1	[i] [lock] [plus] [Service Clients]
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : RS_SubSystem2	[i] [lock] [plus]

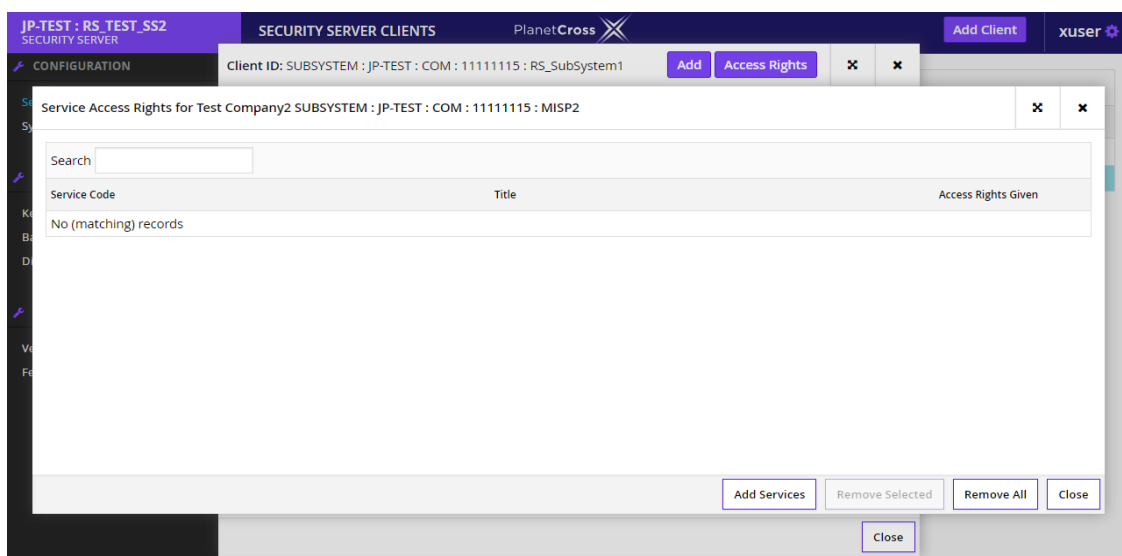
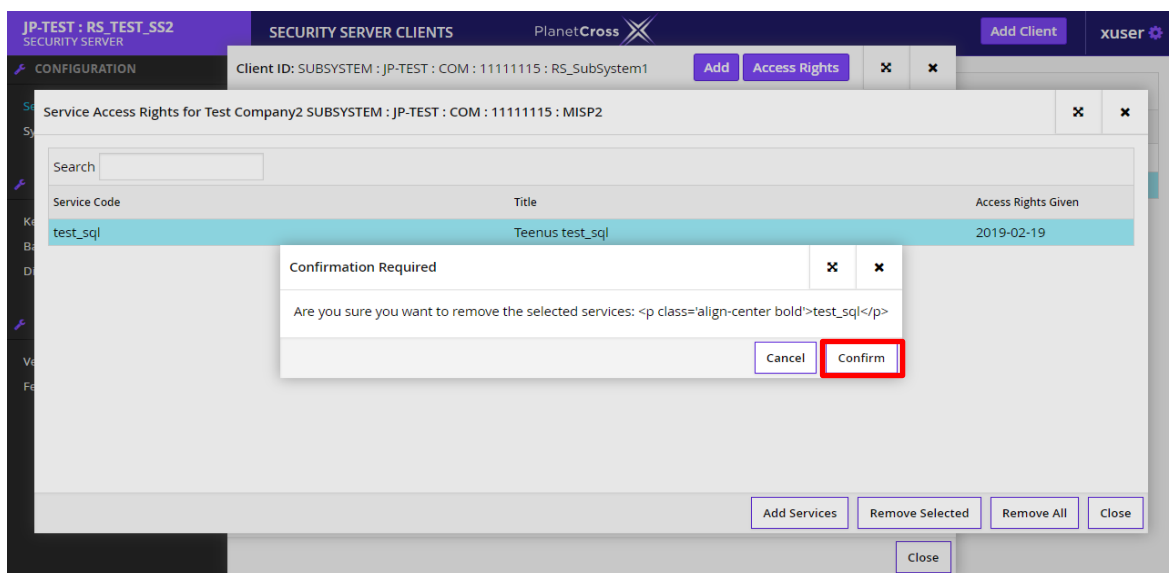
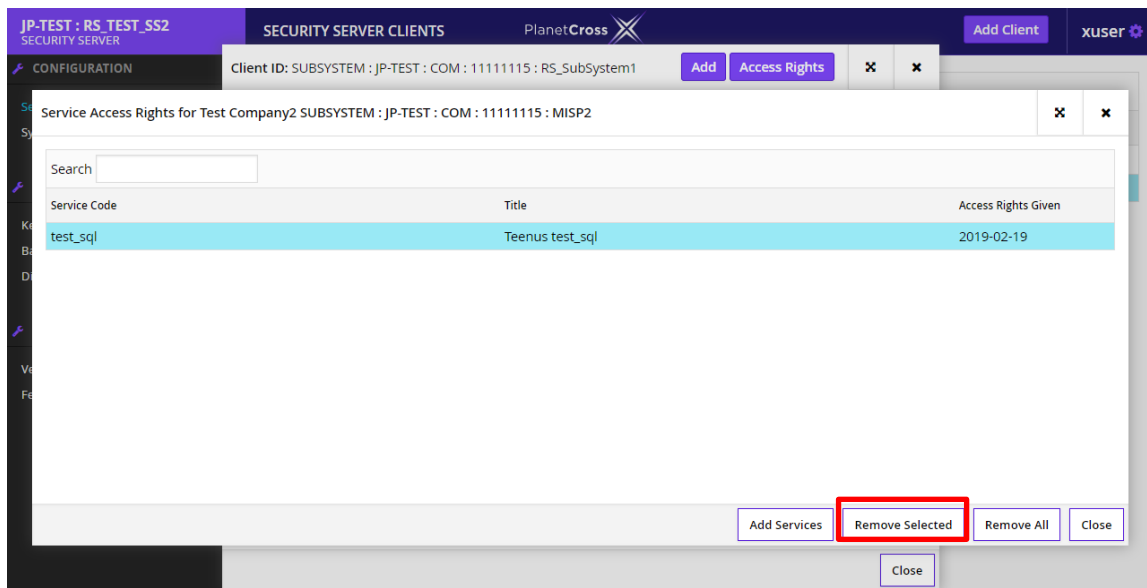
2. In the window that opens, locate and select a subject (a subsystem, or a local or global group) whose access rights you want to change and click **[Access Rights]**.



In the window that opens, a list of services opened in the security server to the selected subject is displayed.



- To remove access rights to a service from the service client, select one or more services from the table and click **[Remove Selected]**, then click **[Confirm]**.



- To remove all access rights from the service client, click **[Remove All]** and then click **[Confirm]**.
- To add access rights to a service client, start by clicking **[Add Service]**. In the window that opens, select the service(s) that you wish to grant to the subject (already granted services are displayed in gray) and click **[Add Selected to ACL]**. To add all services found by the search, click **[Add All to ACL]**.

【Note】

If you refresh the page, all service clients that do not have access rights to any services are removed from the service clients' view.

6.4 Local Access Right Groups

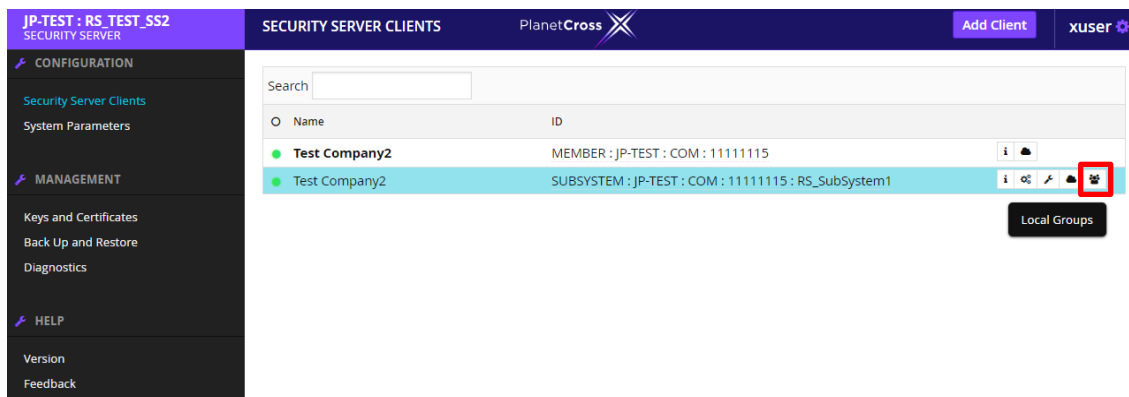
A local access rights group can be created for a security server client in order to facilitate the management of service access rights for a group of PlanetCross subsystems that use the same services. The access rights granted for a group apply for all the members of the group. Local groups are client-based, that is, a local group can only be used to manage the service access rights of one security server client in one security server.

6.5 Adding a Local Group

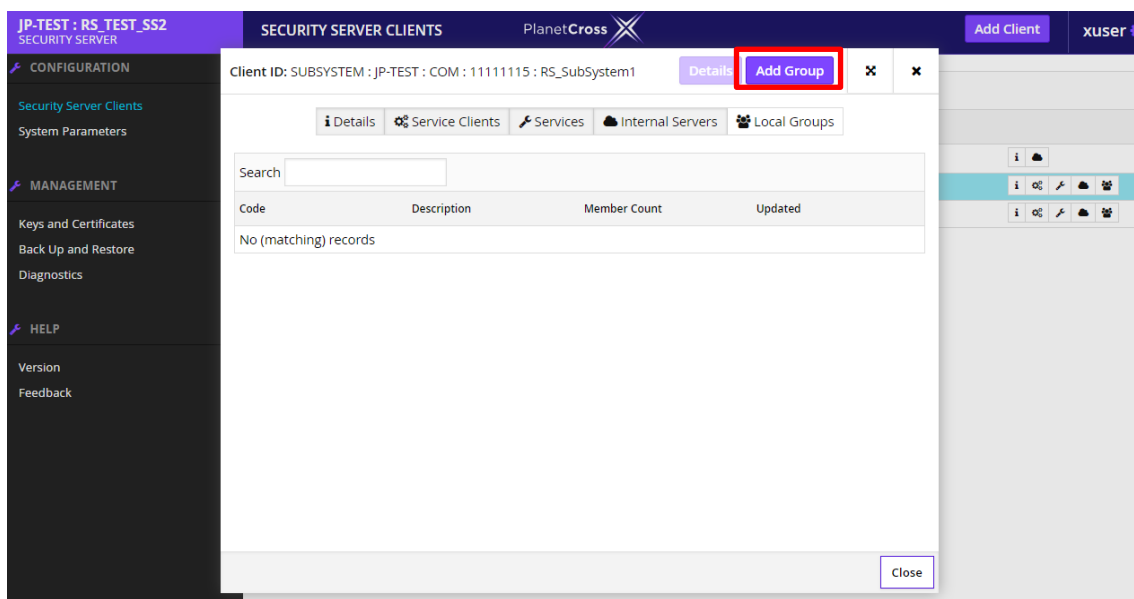
To create a local group for a security server client, follow these steps.

<Access rights: **Service Administrator**>

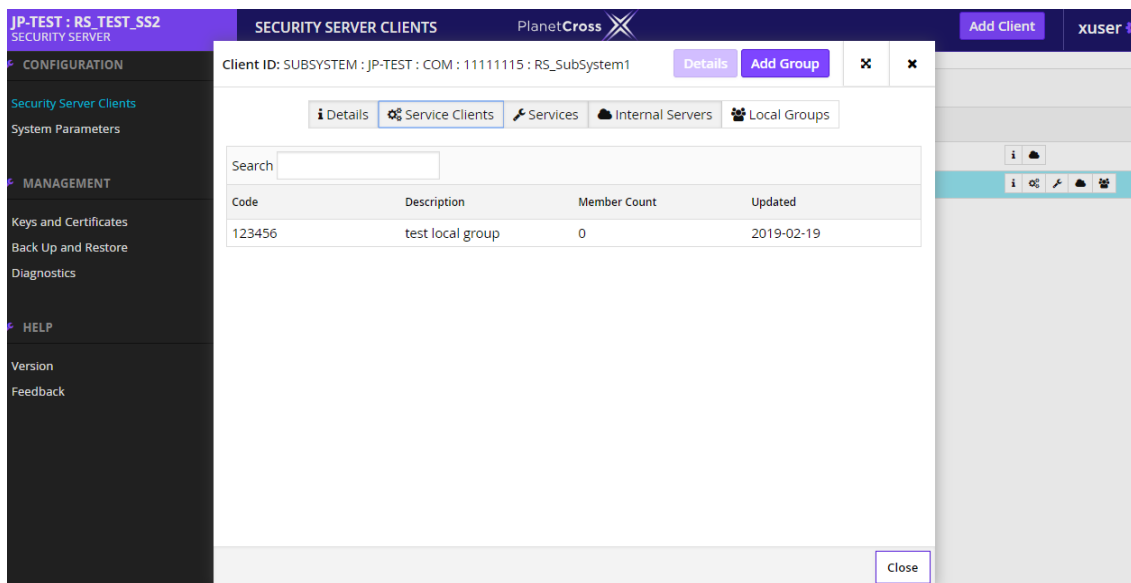
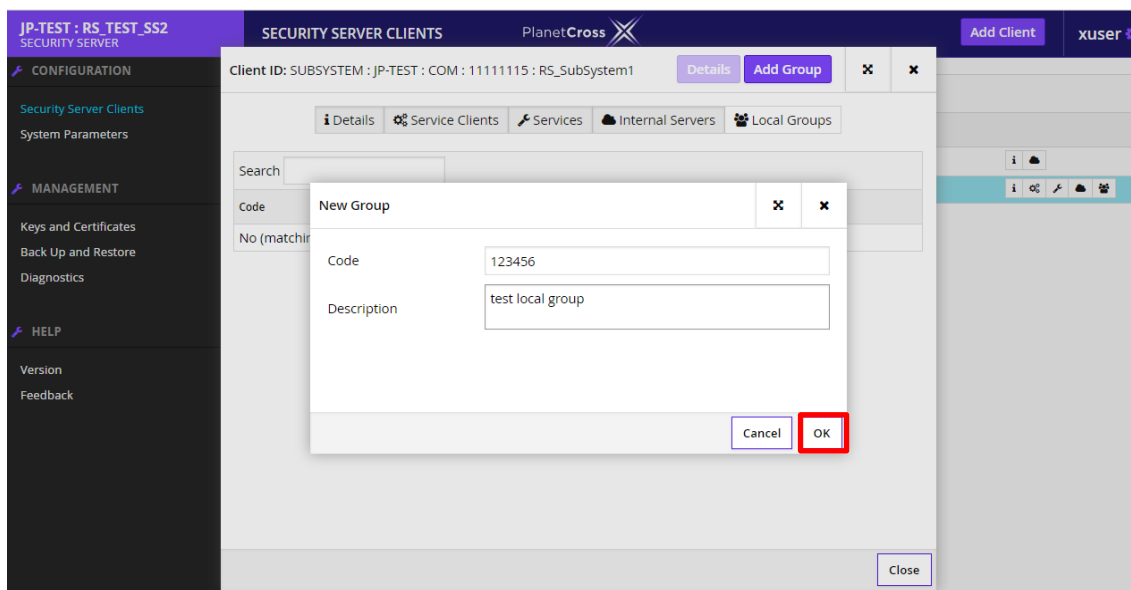
1. On the **[Configuration]** menu, select **[Security Server Clients]**, select a client and click the **[Local Groups]** icon on that row. In the window that opens, a list of the client's local groups is displayed.



2. To create a new group, click **[Add Group]**.



3. In the window that opens, enter the code and description for the new group and click **[OK]**.

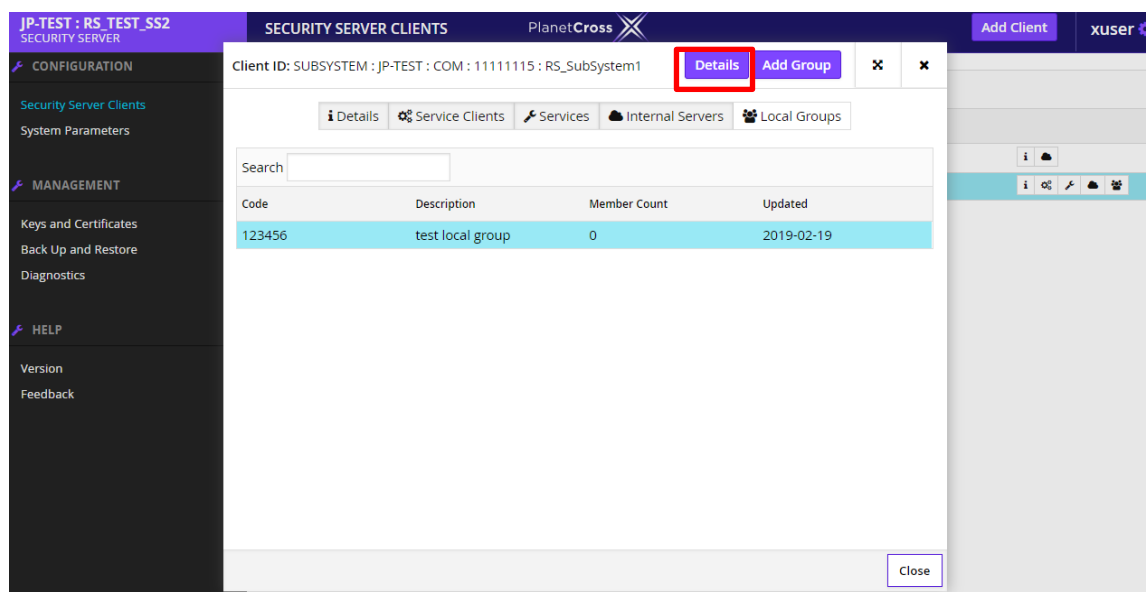


6.6 Displaying and Changing the Members of a Local Group

To view the members of a local group, follow these steps.

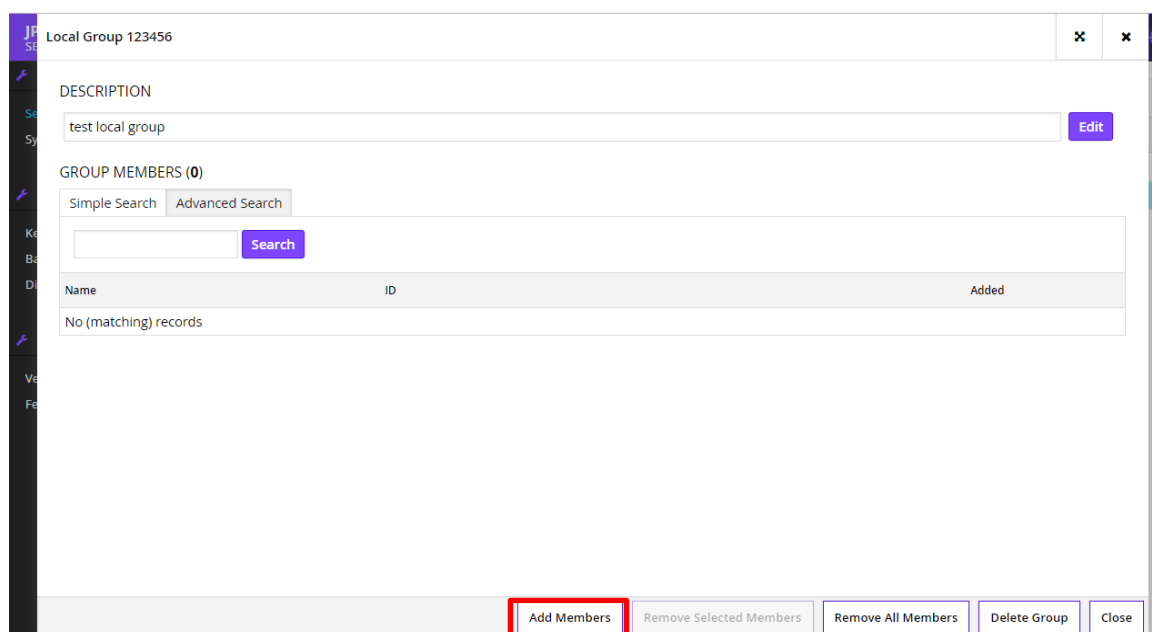
<Access rights: **Service Administrator**>

1. On the **[Configuration]** menu, select **[Security Server Clients]**, select a client and click the **[Local Groups]** icon on that row.
2. In the window that opens, select a group whose members you want to view or change, and click **[Details]** to open the detail view.



To add one or more members to a local group, follow these steps in the group's detail view.

1. Click **[Add Members]**.



2. In the window that opens, locate and select the subsystems that you wish to add to the group and click **[Add Selected to Group]**. To add all subsystems found by the search

function to the group, click **[Add All to Group]**.

Add Members to Local Group 123456

Simple Search Advanced Search

Search

☐ Show group members in search result

Name	ID
No (matching) records	

Add Selected to Group Add All to Group Cancel

Add Members to Local Group 123456

Simple Search Advanced Search

1111115 Search

☐ Show group members in search result

Name	ID
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : KasumiMisp2
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : KasumiTest1
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : KasumiTestSaegusa
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : KasumiTest5
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : KasumiTest3
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : KasumiTest4
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : KasumiTest2
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : MISP2
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : PatientDB
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : PW-azure-DP02-SS-02
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : azure-Train-SP-MISP2-01
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : azure-DP02-RDBA-01_test20181119
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : PW-azure-Manual-SP-SS-01

Add Selected to Group Add All to Group Cancel

Local Group 123456

DESCRIPTION

test local group Edit

GROUP MEMBERS (1)

Simple Search Advanced Search

Search

Name	ID	Added
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : PatientDB	2019-02-19

Add Members Remove Selected Members Remove All Members Delete Group Close

To remove members from a local group, select the members to be deleted in the group's detail view and click **[Remove Selected Members]**. To remove all group members from the group, click **[Remove All Members]**.

Local Group 123456

DESCRIPTION

test local group Edit

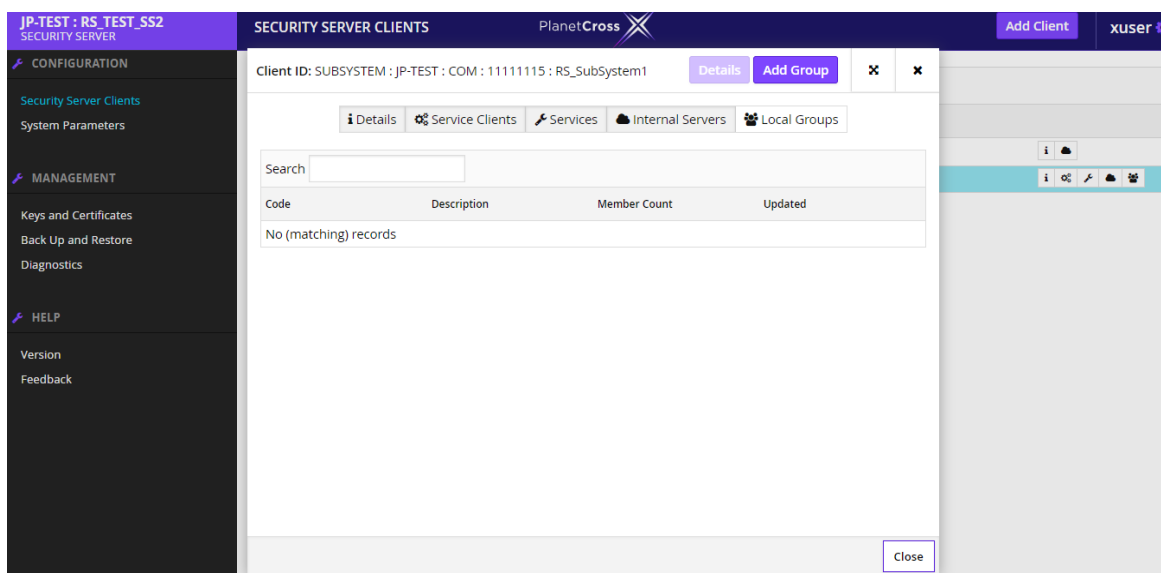
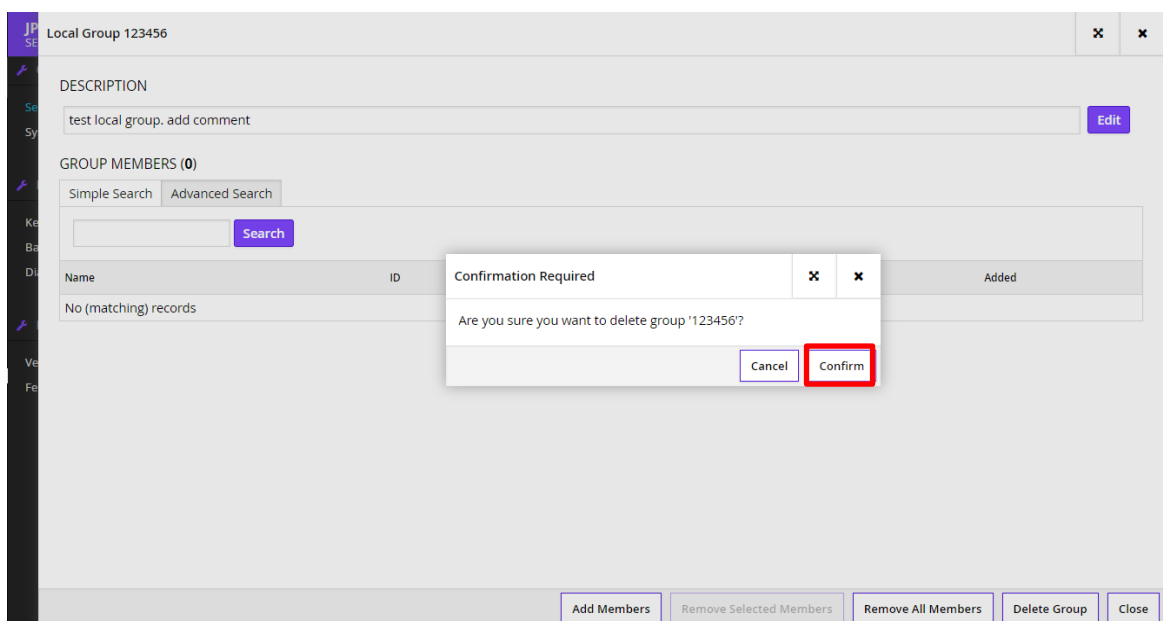
GROUP MEMBERS (1)

Simple Search Advanced Search

Search

Name	ID	Added
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : PatientDB	2019-02-19

Add Members Remove Selected Members Remove All Members Delete Group Close

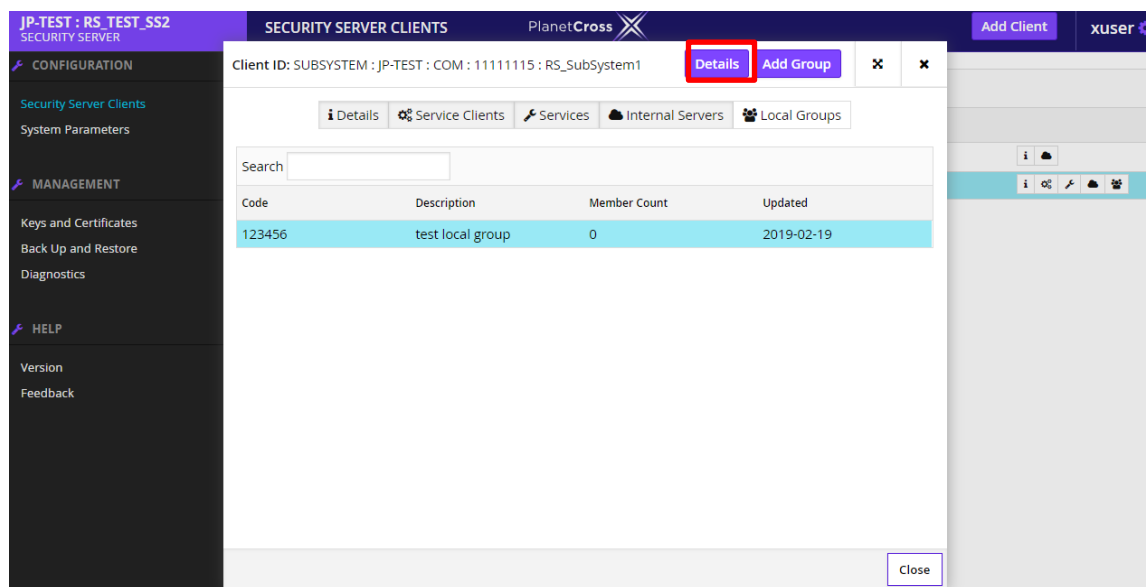


6.7 Changing the description of a Local Group

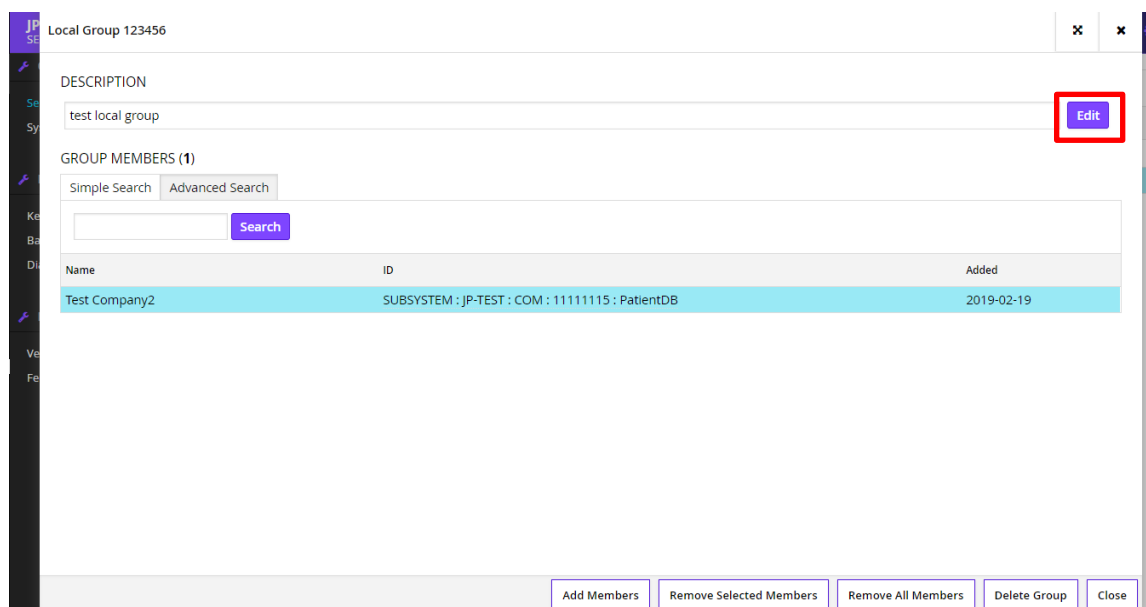
To change the description of a local group, follow these steps.

<Access rights: **Service Administrator**>

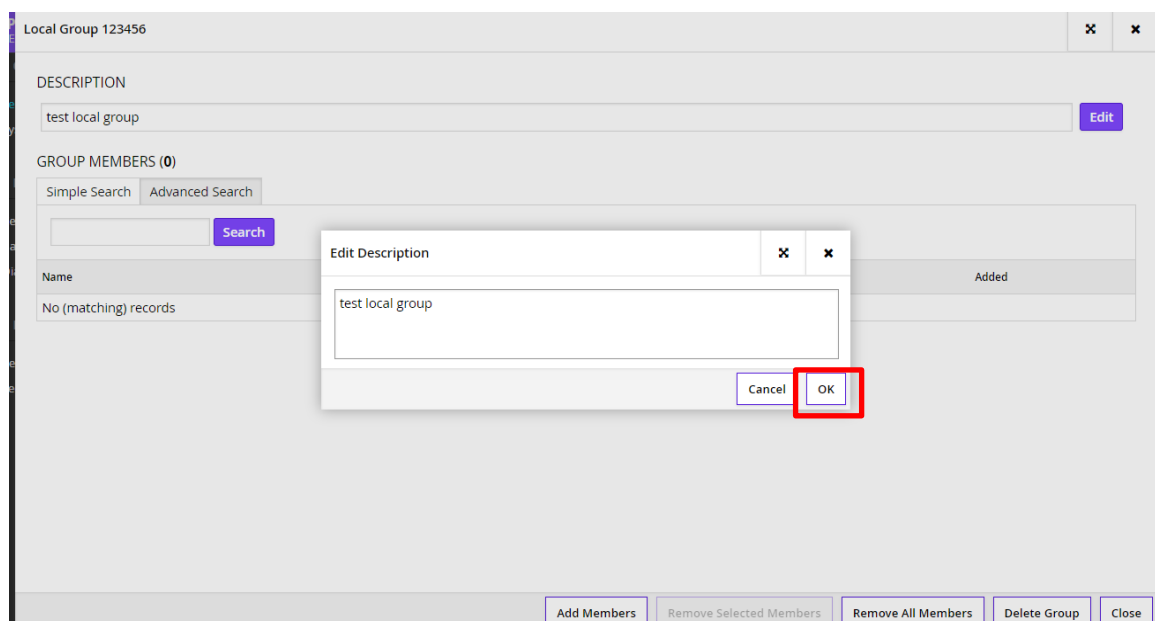
1. On the **[Configuration]** menu, select **[Security Server Clients]**, select a client from the table and click the **[Local Groups]** icon on that row.
2. Select a group from the local groups table and click **[Details]**.



3. In the group detail view, click **[Edit]** to change the description.



4. Enter the group description and click **[OK]**.



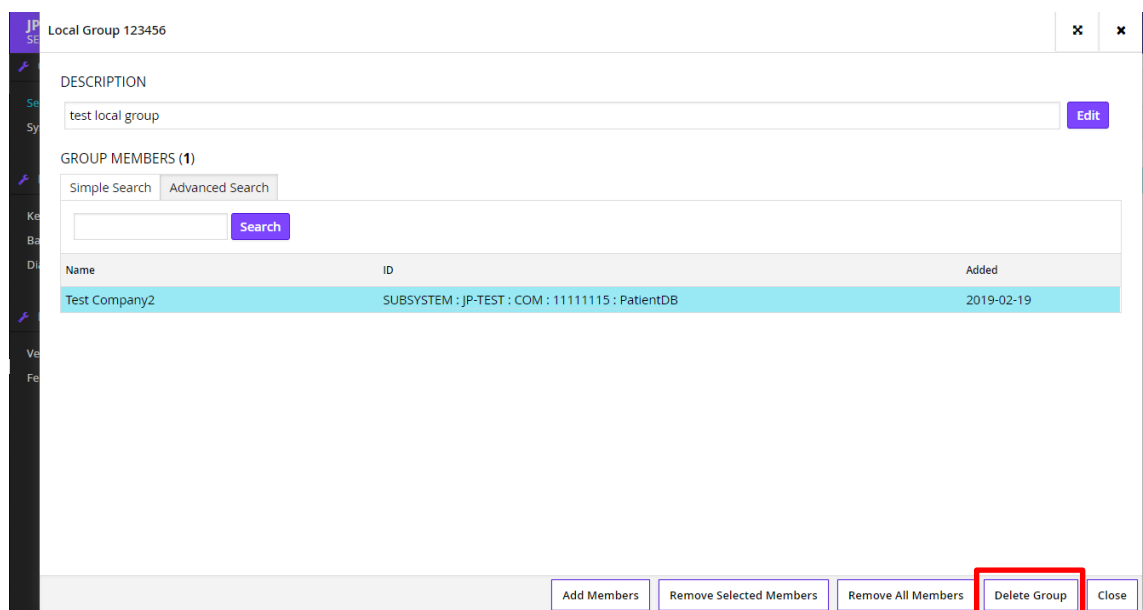
6.8 Deleting a Local Group

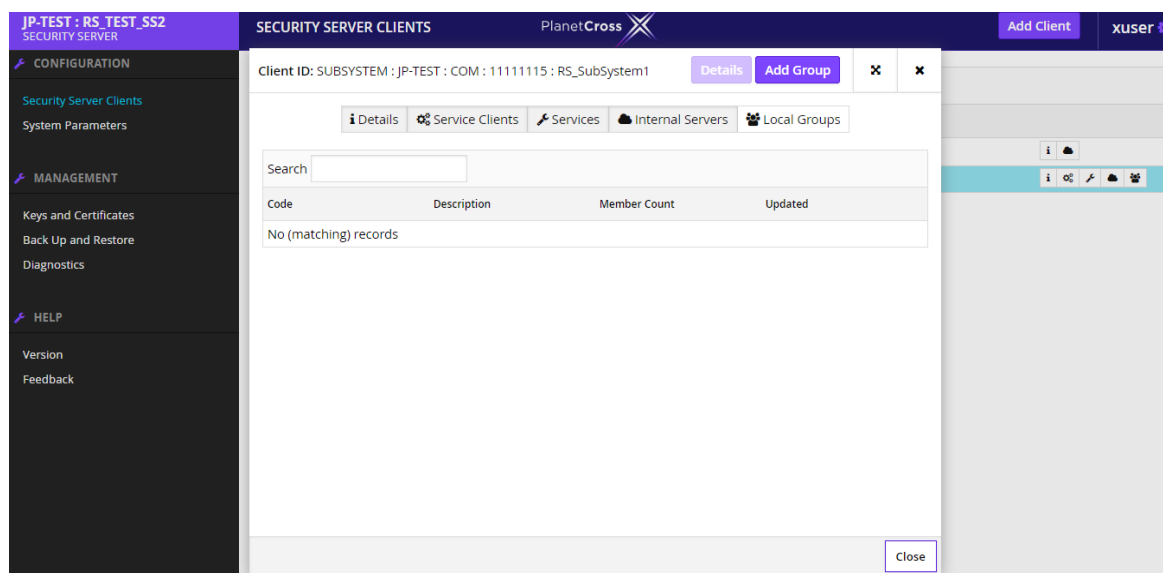
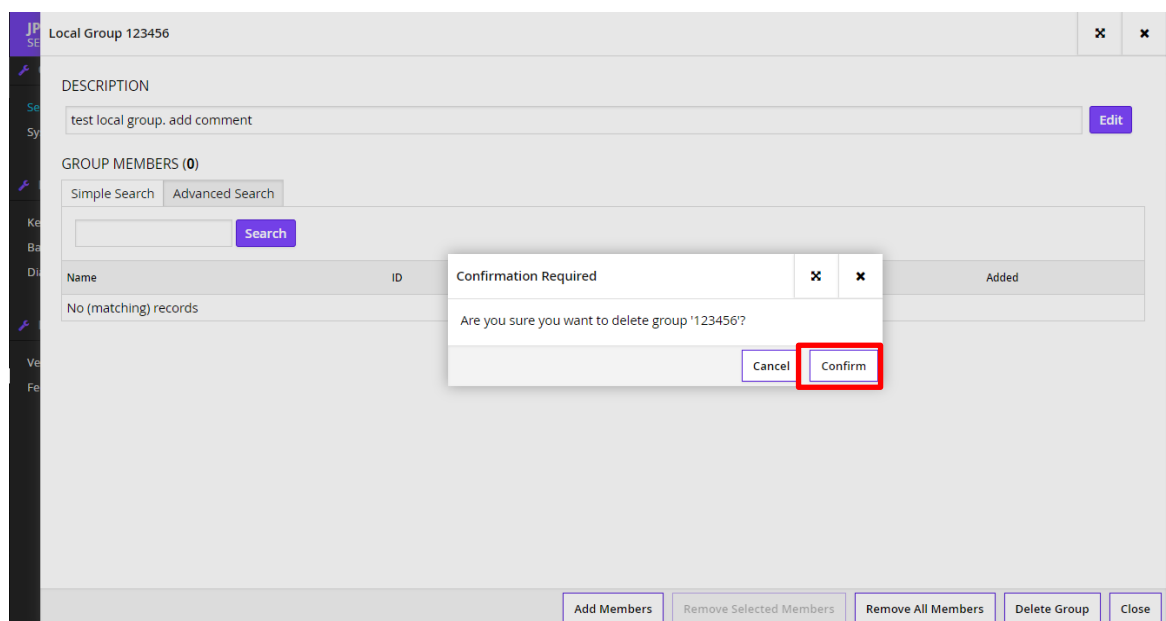
Warning When a local group is deleted, all the group members' access rights, which were granted through belonging to the group, are revoked.

To delete a local group, follow these steps.

<Access rights: **Service Administrator**>

1. On the **[Configuration]** menu, select **[Security Server Clients]**, select a client from the table and click the **[Local Groups]** icon on that row.
2. Select a group from the local groups table and click **[Details]**.
3. In the group detail view, click **[Delete Group]** and confirm the deletion by clicking **[Confirm]** in the window that opens.





7. Communication with the Client Information Systems

A security server can use either the HTTP, HTTPS, or HTTPS NOAUTH protocol to communicate with information system servers which provide and use services.

- The HTTP protocol should be used if the information system server and the security server communicate in a private network segment where no other computers are connected to. Furthermore, the information system server must not allow interactive log-in.
- The HTTPS protocol should be used if it is not possible to provide a separate network segment for the communication between the information system server and the security server. In that case, cryptographic methods are used to protect their communication against potential eavesdropping and interception. Before HTTPS can be used, internal TLS certificates must be created for the information system server(s) and loaded to the security server.
- The HTTPS NOAUTH protocol should be used if you want the security server to skip the verification of the information system TLS certificate.

【Note】

If the HTTP connection method is selected, but the information system connects to the security server over HTTPS, then the connection is accepted, but the client's internal TLS certificate is not verified (same behavior as with HTTPS NOAUTH).

By default the connection type for the security server owner is set to HTTPS to prevent security server clients from making operational monitoring data requests as a security server owner.

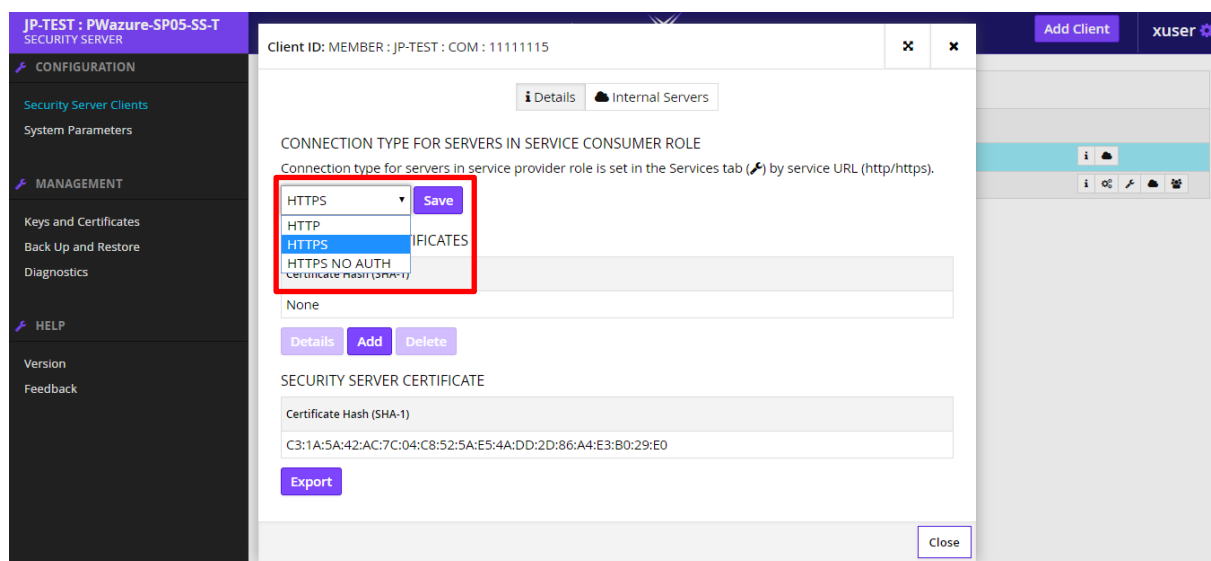
To set the connection method for internal network servers in the service consumer role, follow these steps.

<Access rights: **Service Administrator**>

1. On the **[Configuration]** menu, select **[Security Server Clients]**, select a security server owner or a client from the table and click the **[Internal Servers]** icon on that row.

Name	ID	
Test Company2	MEMBER : JP-TEST : COM : 11111115	
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : RS_SubSystem1	
Test Company2	SUBSYSTEM : JP-TEST : COM : 11111115 : RS_SubSystem2	

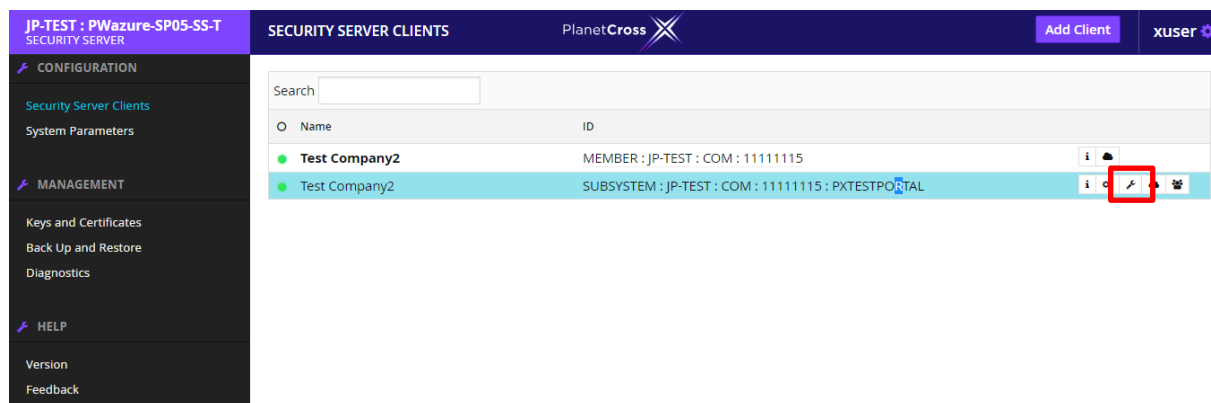
- On the **[Connection Type]** drop-down, select the connection method and click **[Save]**.



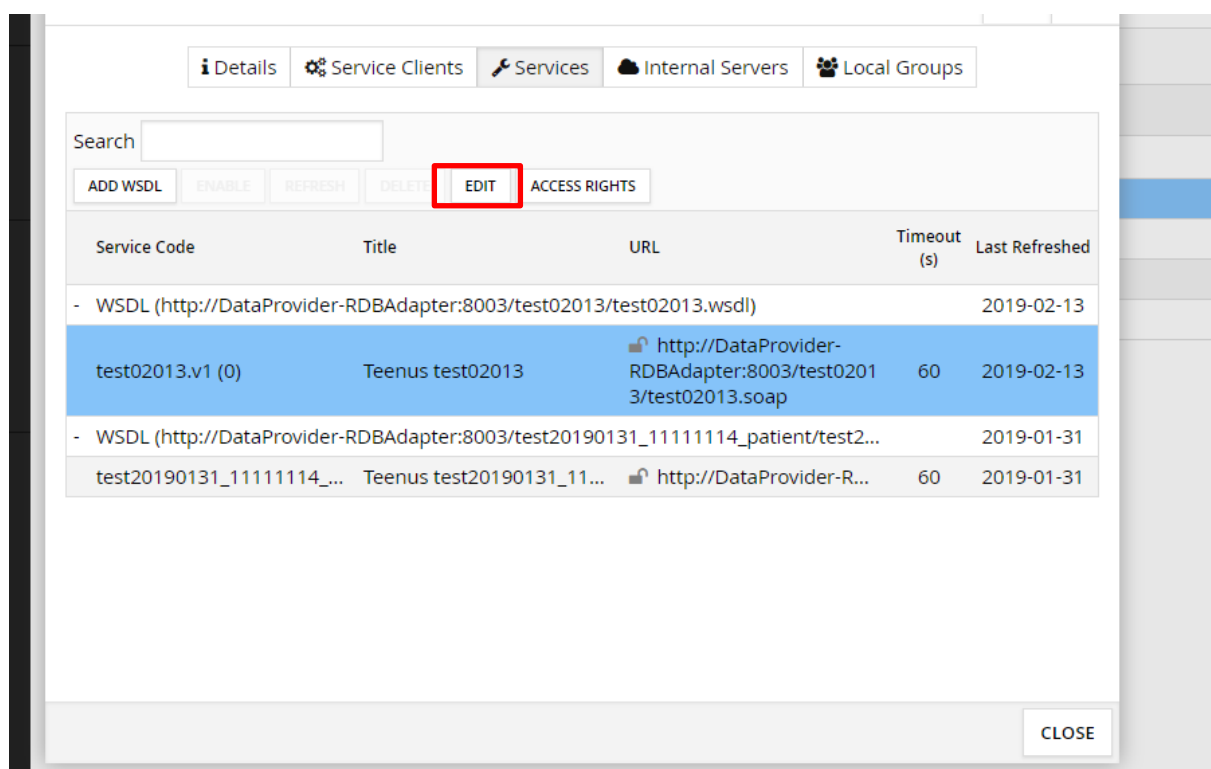
Depending on the configured connection method, the request URL for information system is `http://SECURITYSERVER/` or `https://SECURITYSERVER/`. When making the request, the address SECURITYSERVER must be replaced with the actual address of the security server.

The connection method for internal network servers in the service provider role is determined by the protocol in the URL. To change the connection method, follow these steps.

- On the **[Configuration]** menu, select **[Security Server Clients]**, select a client from the table and click the **[Services]** icon on that row.



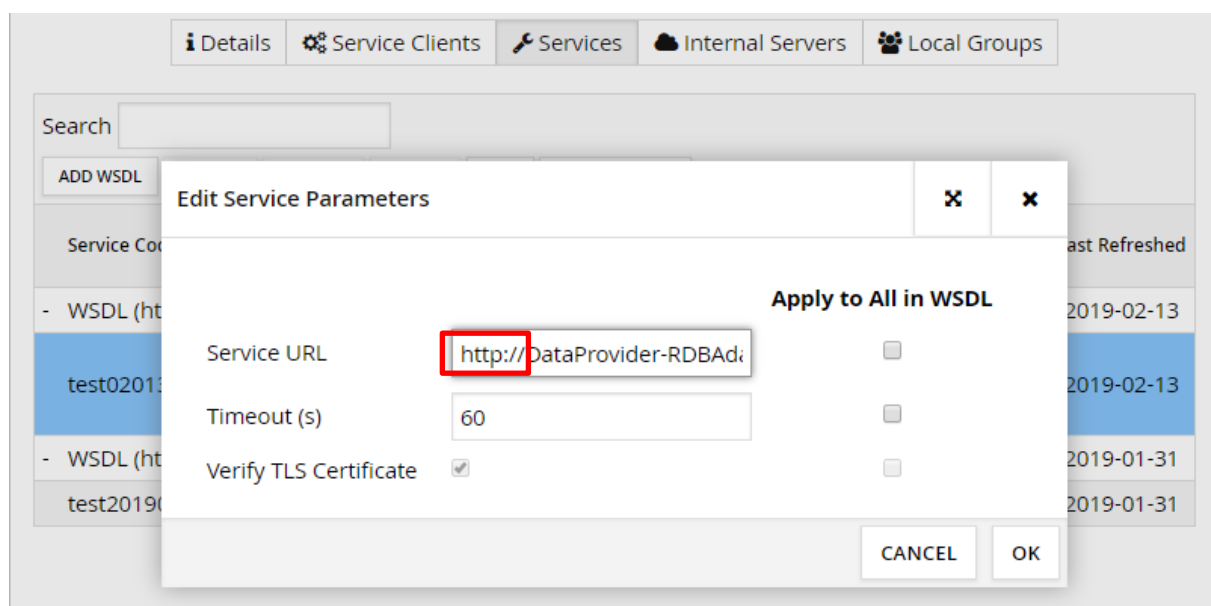
2. Select a service from the table and click **[Edit]**.



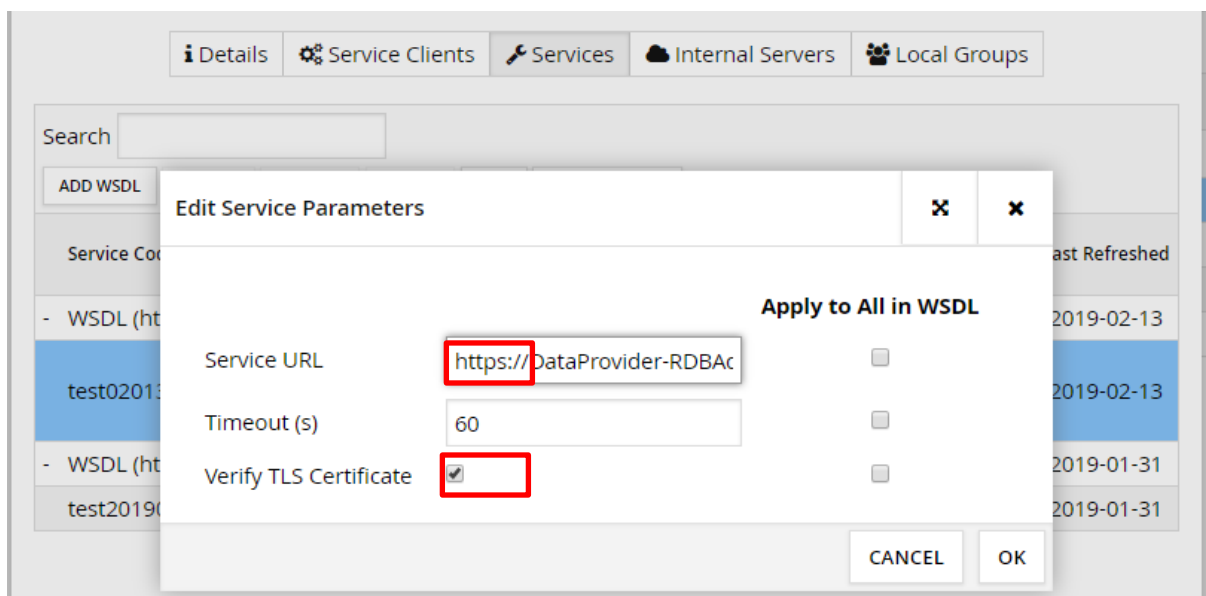
3. Change the protocol in the service URL to HTTP or HTTPS.

If the HTTPS protocol was selected, select the **[Verify TLS certificate]** checkbox if needed. According to the service parameters, the connection with the internal network server is created using one the following protocols:

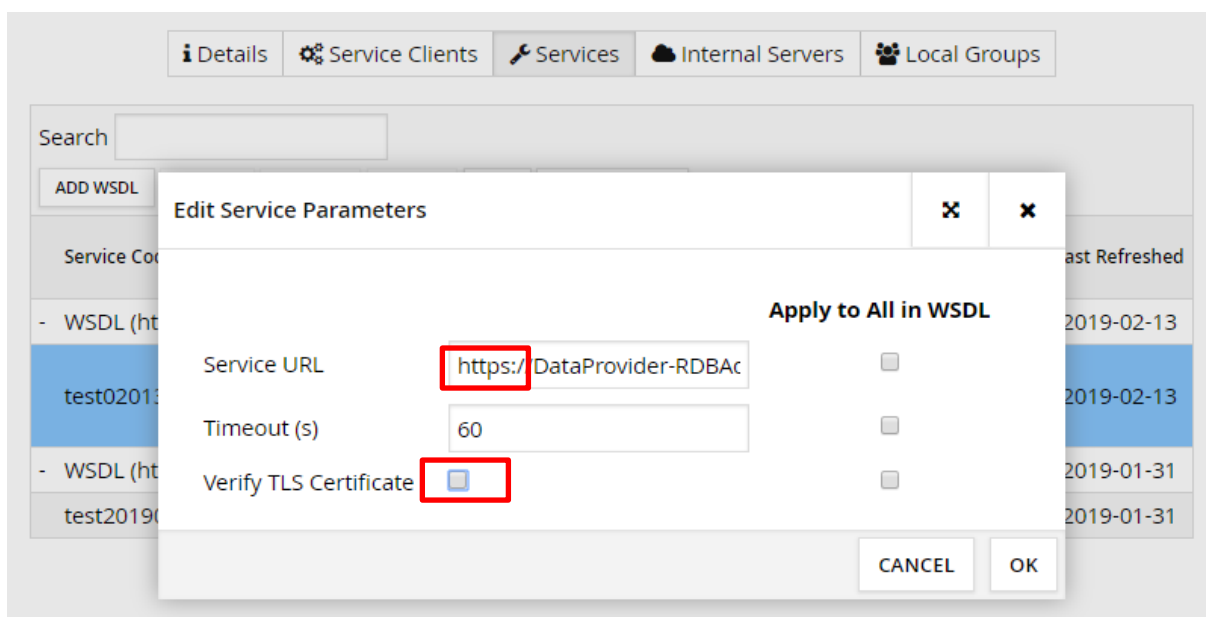
- **HTTP** - the service/adaptor URL begins with "http://...".



- **HTTPS** - the service/adapter URL begins with "https://" and the **[Verify TLS certificate]** checkbox is selected.



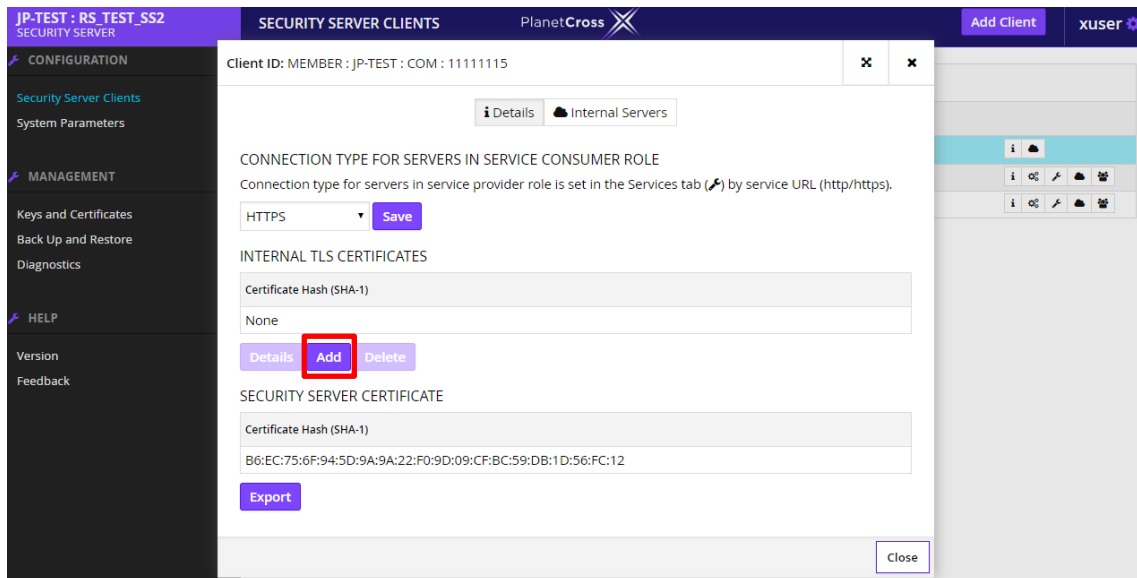
- **HTTPS NOAUTH** - the service/adapter URL begins with "https://" and the **[Verify TLS certificate]** checkbox is not selected.



To add an internal TLS certificate for a security server owner or security server client (for HTTPS connections), follow these steps.

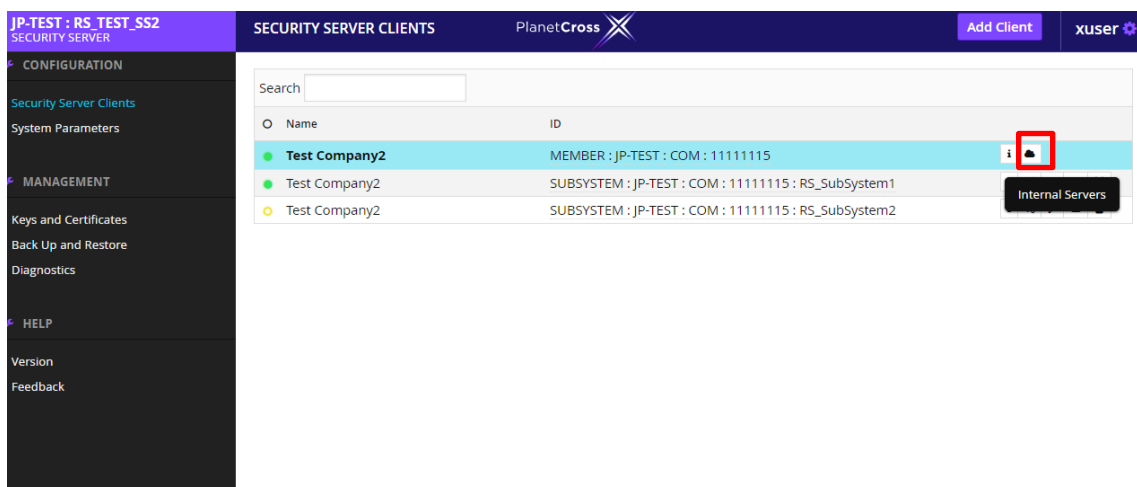
1. On the **[Configuration]** menu, select **[Security Server Clients]**, select a security server owner or a client from the table and click the **[Internal Servers]** icon on that row.

- To add a certificate, click **[Add]** in the **[Internal TLS Certificates]** section, select a certificate file from the local file system and click **[OK]**.
The certificate fingerprint appears in the “**Internal TLS Certificates**” table.

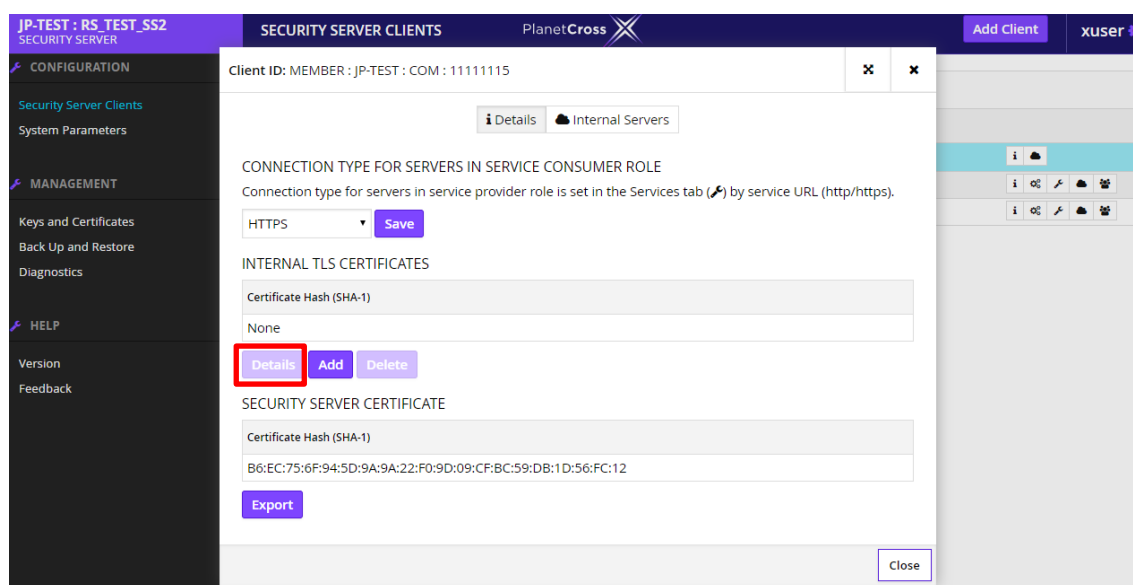


To display the detailed information of an internal TLS certificate, follow these steps.

- On the **[Configuration]** menu, select **[Security Server Clients]**, select a security server owner or a client from the table and click the **[Internal Servers]** icon on that row.

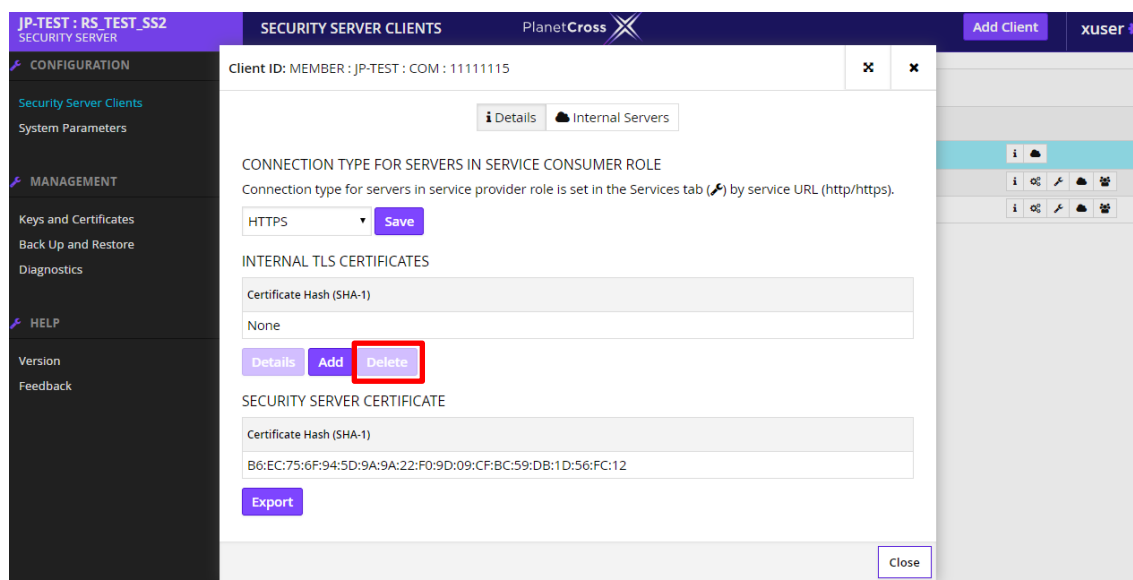


2. Select a certificate from the “**Internal TLS Certificates**” table and click **[Details]**.



To delete an internal TLS certificate, follow these steps.

1. On the **[Configuration]** menu, select **[Security Server Clients]**, select a security server owner or a client from the table and click the **[Internal Servers]** icon on that row.
2. Select a certificate from the “**Internal TLS Certificates**” table and click **[Delete]**.

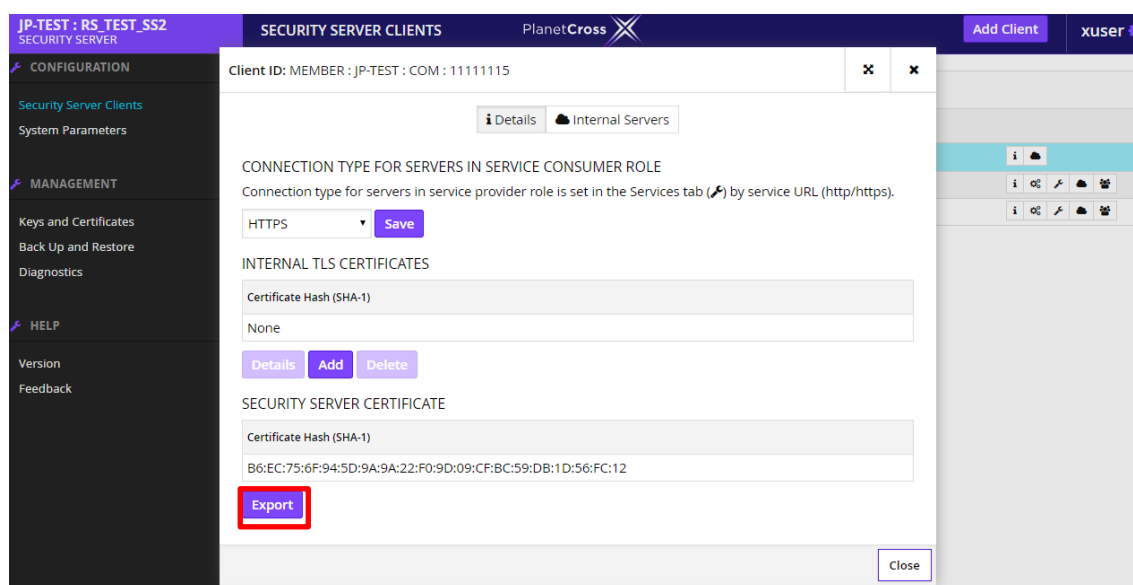


3. Confirm the deletion by clicking **[Confirm]** in the window that opens.

To export the security server's internal TLS certificate, follow these steps.

1. On the **[Configuration]** menu, select **[Security Server Clients]**, select a security server owner or a client from the table and click the **[Internal Servers]** icon on that row.

2. Click **[Export]** and save the prompted file to the local file system.



8. System Parameters

The security server system parameters are:

- **Configuration anchor's information** - The configuration anchor contains data that is used to periodically download signed configuration from the central server and to verify the signature of the downloaded configuration.
- **Timestamping service information** - Timestamping is used to preserve the evidential value of messages exchanged over PlanetCross.
- **The internal TLS key and certificate** - The internal TLS certificate is used to establish a TLS connection with the security server client's information system if the "HTTPS" connection method is chosen for the client's servers.

8.1 Managing the Configuration Anchor

To upload the configuration anchor, follow these steps.

<Access rights : For uploading the configuration anchor: **Security Officer**>

<Access rights : For downloading the configuration anchor: **Security Officer , System Administrator**>

1. On the **[Configuration]** menu, select **[System Parameters]**. The system parameters view is opened.
2. In the **[Configuration Anchor]** section, click **[Upload]**.

Configuration Anchor

Hash (SHA-224): 28:A9:8F:F2:E4:29:3E:4D:98:8B:52:5D:66:67:EB:15:F4:04:D1:AE:42:BE:9F:0F:F8:62:6E:09
Generated: UTC 2017-10-16 22:20:17

Timestamping Services

Timestamping service	Service URL
Planetway Timestamping Authority	https://tsa.avenuecross.com

Approved Certificate Authorities

Distinguished Name	OCSP response	Expires
/C=EE/O=Planetway Europe OÜ/CN=Planetway Avenue Cross Root CA	N/A	2037-07-03
/C=EE/O=Planetway Europe OÜ/OU=Issuing CA/CN=Planetway Avenue Cross Issuing CA	good	2037-07-03
/C=JP/O=TEIKOKU DATA BANK, LTD./OU=TDB CA SAO/CN=TDB CA for Signature and Au...	N/A	2027-12-03

Internal TLS Certificate

Certificate hash (SHA-1): B6:EC:75:6F:94:5D:9A:9A:22:F0:9D:09:CF:BC:59:DB:1D:56:FC:12

3. Find the anchor file from the local file system and click **[Upload]**.
4. Ensure that the anchor file you are uploading is valid by comparing the hash value of the uploaded file with the hash value of the currently valid anchor published by the PlanetCross governing authority. If the hash values match, confirm the upload by clicking **[Confirm]**.

To download the configuration anchor, follow these steps.

1. On the **[Configuration]** menu, select **[System Parameters]**. The system parameters view is opened.

- On the **[Configuration Anchor]** section, click **[Download]** and save the prompted file.

JP-TEST : RS_TEST_SS2
SECURITY SERVER

SYSTEM PARAMETERS PlanetCross xuser

Configuration Anchor [Download] [Upload]

Hash (SHA-224): 28:A9:8F:F2:E4:29:3E:4D:98:8B:52:5D:66:67:EB:15:F4:04:D1:AE:42:BE:9F:0F:F8:62:6E:09
Generated: UTC 2017-10-16 22:20:17

Timestamping Services [Delete] [Add]

Timestamping service	Service URL
Planetway Timestamping Authority	https://tsa.avenuecross.com

Approved Certificate Authorities

Distinguished Name	OCSP response	Expires
/C=EE/O=Planetway Europe OÜ/CN=Planetway Avenue Cross Root CA	N/A	2037-07-03
/C=EE/O=Planetway Europe OÜ/OU=Issuing CA/CN=Planetway Avenue Cross Issuing CA	good	2037-07-03
/C=JP/O=TEIKOKU DATA BANK, LTD./OU=TDB CA SAO/CN=TDB CA for Signature and Au...	N/A	2027-12-03

Internal TLS Certificate [Generate New TLS Key] [Generate Certificate Request] [Import] [Export] [Certificate Details]

Certificate hash (SHA-1): B6:EC:75:6F:94:5D:9A:9A:22:F0:9D:09:CF:BC:59:DB:1D:56:FC:12

8.2 Managing the Timestamping Services

To add a timestamping service, follow these steps.

<Access rights: **Security Officer**>

- On the **[Configuration]** menu, select **[System Parameters]**. The system parameters view is opened.
- In the Timestamping Services section, click **[Add]**.

JP-TEST : RS_TEST_SS2
SECURITY SERVER

SYSTEM PARAMETERS PlanetCross xuser

Configuration Anchor [Download] [Upload]

Hash (SHA-224): 28:A9:8F:F2:E4:29:3E:4D:98:8B:52:5D:66:67:EB:15:F4:04:D1:AE:42:BE:9F:0F:F8:62:6E:09
Generated: UTC 2017-10-16 22:20:17

Timestamping Services [Delete] [Add]

Timestamping service	Service URL
Planetway Timestamping Authority	https://tsa.avenuecross.com

Approved Certificate Authorities

Distinguished Name	OCSP response	Expires
/C=EE/O=Planetway Europe OÜ/CN=Planetway Avenue Cross Root CA	N/A	2037-07-03
/C=EE/O=Planetway Europe OÜ/OU=Issuing CA/CN=Planetway Avenue Cross Issuing CA	good	2037-07-03
/C=JP/O=TEIKOKU DATA BANK, LTD./OU=TDB CA SAO/CN=TDB CA for Signature and Au...	N/A	2027-12-03

Internal TLS Certificate [Generate New TLS Key] [Generate Certificate Request] [Import] [Export] [Certificate Details]

Certificate hash (SHA-1): B6:EC:75:6F:94:5D:9A:9A:22:F0:9D:09:CF:BC:59:DB:1D:56:FC:12

- In the window that opens, select a service and click **[OK]**.

To delete a timestamping service, follow these steps.

1. On the **[Configuration]** menu, select **[System Parameters]**. The system parameters view is opened.
2. In the **[Timestamping Services]** section, select the service to be deleted and click **[Delete]**.

JP-TEST : RS_TEST_SS2
SECURITY SERVER

SYSTEM PARAMETERS PlanetCross xuser

CONFIGURATION

- Security Server Clients
- System Parameters**

MANAGEMENT

- Keys and Certificates
- Back Up and Restore
- Diagnostics

HELP

- Version
- Feedback

Configuration Anchor [Download] [Upload]

Hash (SHA-224): 28:A9:8F:F2:E4:29:3E:4D:98:8B:52:5D:66:67:EB:15:F4:04:D1:AE:42:BE:9F:0F:F8:62:6E:09
Generated: UTC 2017-10-16 22:20:17

Timestamping Services [Delete] [Add]

Timestamping service	Service URL
Planetway Timestamping Authority	https://tsa.avenuecross.com

Approved Certificate Authorities

Distinguished Name	OCSP response	Expires
/C=EE/O=Planetway Europe OÜ/CN=Planetway Avenue Cross Root CA	N/A	2037-07-03
/C=EE/O=Planetway Europe OÜ/OU=Issuing CA/CN=Planetway Avenue Cross Issuing CA	good	2037-07-03
/C=JP/O=TEIKOKU DATA BANK, LTD./OU=TDB CA SAO/CN=TDB CA for Signature and Au...	N/A	2027-12-03

Internal TLS Certificate [Generate New TLS Key] [Generate Certificate Request] [Import] [Export] [Certificate Details]

Certificate hash (SHA-1): B6:EC:75:6F:94:5D:9A:9A:22:F0:9D:09:CF:BC:59:DB:1D:56:FC:12

【Note】

If more than one time stamping service is configured, the security server will try to get a timestamp from the topmost service in the table, moving down to the next service if the try was unsuccessful.

8.3 Changing the Internal TLS Key and Certificate

To change the security server's internal TLS key and certificate , follow these steps.

<Access rights: **Security Officer** , **System Administrator**>

1. On the **[Configuration]** menu, select **[System Parameters]**. The system parameters view is opened.
2. In the **[Internal TLS Certificate]** section, click **[Generate New TLS Key]** and in the window that opens, click **[Confirm]**.

JP-TEST : RS_TEST_SS2
SECURITY SERVER

SYSTEM PARAMETERS PlanetCross xuser

CONFIGURATION

- Security Server Clients
- System Parameters

MANAGEMENT

- Keys and Certificates
- Back Up and Restore
- Diagnostics

HELP

- Version
- Feedback

Configuration Anchor Download Upload

Hash (SHA-224): 28:A9:8F:F2:E4:29:3E:4D:98:8B:52:5D:66:67:EB:15:F4:04:D1:AE:42:BE:9F:0F:F8:62:6E:09
Generated: UTC 2017-10-16 22:20:17

Timestamping Services Delete Add

Timestamping service	Service URL
Planetway Timestamping Authority	https://tsa.avenuecross.com

Approved Certificate Authorities

Distinguished Name	OCSP response	Expires
/C=EE/O=Planetway Europe OÜ/CN=Planetway Avenue Cross Root CA	N/A	2037-07-03
/C=EE/O=Planetway Europe OÜ/OU=Issuing CA/CN=Planetway Avenue Cross Issuing CA	good	2037-07-03
/C=JP/O=TEIKOKU DATA BANK, LTD./OU=TDB CA SAO/CN=TDB CA for Signature and Au...	N/A	2027-12-03

Internal TLS Certificate Generate Certificate Request Import Export Certificate Details

Generate New TLS Key

Certificate hash (SHA-1): B6:EC:75:6F:94:5D:9A:9A:22:F0:9D:09:CF:BC:59:DB:1D:56:FC:12

The security server generates a key used for communication with the client information systems, and the corresponding self-signed certificate. The security server's certificate fingerprint will also change. The security server's domain name is saved to the certificate's Common Name field, and the internal IP address to the subjectAltName extension field.

To generate a new certificate request , follow these steps.

1. On the **[Configuration]** menu, select **[System Parameters]**. The system parameters view is opened.
2. In the **“Internal TLS Certificate”** section, click **[Generate Certificate Request]**, input the Distinguished Name and save the certificate request file to the local file system.

JP-TEST : RS_TEST_SS2
SECURITY SERVER

SYSTEM PARAMETERS PlanetCross

CONFIGURATION

- Security Server Clients
- System Parameters

MANAGEMENT

- Keys and Certificates
- Back Up and Restore
- Diagnostics

HELP

- Version
- Feedback

Configuration Anchor [Download] [Upload]

Hash (SHA-224): 28:A9:8F:F2:E4:29:3E:4D:98:8B:52:5D:66:67:EB:15:F4:04:D1:AE:42:BE:9F:0F:F8:62:6E:09
Generated: UTC 2017-10-16 22:20:17

Timestamping Services [Delete] [Add]

Timestamping service	Service URL
Planetway Timestamping Authority	https://tsa.avenuecross.com

Approved Certificate Authorities

Distinguished Name	OCSP response	Expires
/C=EE/O=Planetway Europe OÜ/CN=Planetway Avenue Cross Root CA	N/A	2037-07-03
/C=EE/O=Planetway Europe OÜ/OU=Issuing CA/CN=Planetway Avenue Cross Issuing CA	good	2037-07-03
/C=JP/O=TEIKOKU DATA BANK, LTD./OU=TDB CA SAO/CN=TDB CA for Signature and Au...	N/A	2027-12-03

Internal TLS Certificate [Generate New TLS Key] **Generate Certificate Request** [Import] [Export] [Certificate Details]

Certificate hash (SHA-1): B6:EC:75:6F:94:5D:9A:9A:22:F0:9D:09:CF:BC:59:DB:1D:56:FC:12

The security server generates a certificate request using the current key and the provided Distinguished Name.

To import a new TLS certificate , follow these steps.

1. On the **[Configuration]** menu, select **[System Parameters]**. The system parameters view is opened.
2. In the **[Internal TLS Certificate]** section, click **[Import]** and point to the file to be imported.

JP-TEST : RS_TEST_SS2
SECURITY SERVER

SYSTEM PARAMETERS PlanetCross

CONFIGURATION

- Security Server Clients
- System Parameters

MANAGEMENT

- Keys and Certificates
- Back Up and Restore
- Diagnostics

HELP

- Version
- Feedback

Configuration Anchor [Download] [Upload]

Hash (SHA-224): 28:A9:8F:F2:E4:29:3E:4D:98:8B:52:5D:66:67:EB:15:F4:04:D1:AE:42:BE:9F:0F:F8:62:6E:09
Generated: UTC 2017-10-16 22:20:17

Timestamping Services [Delete] [Add]

Timestamping service	Service URL
Planetway Timestamping Authority	https://tsa.avenuecross.com

Approved Certificate Authorities

Distinguished Name	OCSP response	Expires
/C=EE/O=Planetway Europe OÜ/CN=Planetway Avenue Cross Root CA	N/A	2037-07-03
/C=EE/O=Planetway Europe OÜ/OU=Issuing CA/CN=Planetway Avenue Cross Issuing CA	good	2037-07-03
/C=JP/O=TEIKOKU DATA BANK, LTD./OU=TDB CA SAO/CN=TDB CA for Signature and Au...	N/A	2027-12-03

Internal TLS Certificate [Generate New TLS Key] [Generate Certificate Request] **Import** [Export] [Certificate Details]

Certificate hash (SHA-1): B6:EC:75:6F:94:5D:9A:9A:22:F0:9D:09:CF:BC:59:DB:1D:56:FC:12

【Note】

The imported certificate must be in PEM-format to be accepted. Certificate chains are supported; concatenate possible intermediate certificate(s) to the server certificate before importing the file. that importing a new TLS certificate will restart the xroad-proxy and thus affects providing services from the security server.

To export the security server's internal TLS certificate , follow these steps.

1. On the **[Configuration]** menu, select **[System Parameters]**. The system parameters view is opened.
2. In the **[Internal TLS Certificate]** section, click **[Export]** and save the prompted file to the local file system.

The screenshot shows the PlanetCross Security Server configuration interface. The left sidebar contains a menu with 'CONFIGURATION' selected, and 'System Parameters' is highlighted. The main content area is titled 'SYSTEM PARAMETERS' and includes sections for 'Configuration Anchor', 'Timestamping Services', 'Approved Certificate Authorities', and 'Internal TLS Certificate'. In the 'Internal TLS Certificate' section, the 'Export' button is highlighted with a red box.

Configuration Anchor

Hash (SHA-224): 28:A9:8F:F2:E4:29:3E:4D:98:8B:52:5D:66:67:EB:15:F4:04:D1:AE:42:BE:9F:0F:F8:62:6E:09
Generated: UTC 2017-10-16 22:20:17

Timestamping Services

Timestamping service	Service URL
Planetway Timestamping Authority	https://tsa.avenuecross.com

Approved Certificate Authorities

Distinguished Name	OCSP response	Expires
/C=EE/O=Planetway Europe OÜ/CN=Planetway Avenue Cross Root CA	N/A	2037-07-03
/C=EE/O=Planetway Europe OÜ/OU=Issuing CA/CN=Planetway Avenue Cross Issuing CA	good	2037-07-03
/C=JP/O=TEIKOKU DATA BANK, LTD./OU=TDB CA SAO/CN=TDB CA for Signature and Au...	N/A	2027-12-03

Internal TLS Certificate

Generate New TLS Key Generate Certificate Request Import **Export** Certificate Details

Certificate hash (SHA-1): B6:EC:75:6F:94:5D:9A:9A:22:F0:9D:09:CF:BC:59:DB:1D:56:FC:12

【Note】

That only the internal server certificate is exported, not the possible intermediate certificates.

To view the detailed information of the security server's internal TLS certificate , follow these steps.

1. On the **[Configuration]** menu, select **[System Parameters]**. The system parameters view is opened.
2. In the **[Internal TLS Certificate]** section, click **[Certificate Details]**.

The screenshot shows the PlanetCross Security Server configuration interface, identical to the previous one. In the 'Internal TLS Certificate' section, the 'Certificate Details' button is highlighted with a red box.

Configuration Anchor

Hash (SHA-224): 28:A9:8F:F2:E4:29:3E:4D:98:8B:52:5D:66:67:EB:15:F4:04:D1:AE:42:BE:9F:0F:F8:62:6E:09
Generated: UTC 2017-10-16 22:20:17

Timestamping Services

Timestamping service	Service URL
Planetway Timestamping Authority	https://tsa.avenuecross.com

Approved Certificate Authorities

Distinguished Name	OCSP response	Expires
/C=EE/O=Planetway Europe OÜ/CN=Planetway Avenue Cross Root CA	N/A	2037-07-03
/C=EE/O=Planetway Europe OÜ/OU=Issuing CA/CN=Planetway Avenue Cross Issuing CA	good	2037-07-03
/C=JP/O=TEIKOKU DATA BANK, LTD./OU=TDB CA SAO/CN=TDB CA for Signature and Au...	N/A	2027-12-03

Internal TLS Certificate

Generate New TLS Key Generate Certificate Request Import Export **Certificate Details**

Certificate hash (SHA-1): B6:EC:75:6F:94:5D:9A:9A:22:F0:9D:09:CF:BC:59:DB:1D:56:FC:12

9. Message Log

The purpose of the message log is to provide means to prove the reception of a regular request or response message to a third party. Messages exchanged between security servers are signed and encrypted. For every regular request and response, the security server produces a complete signed and timestamped document (Associated Signature Container [ASiC]).

Message log data is stored to the database of the security server during message exchange. According to the configuration, the timestamping of the signatures of the exchanged messages is either synchronous to the message exchange process or is done asynchronously using the time period set by the PlanetCross governing agency.

In case of synchronous timestamping, the timestamping is an integral part of the message exchange process (one timestamp is taken for the request and another for the response). If the timestamping fails, the message exchange fails as well and the security server responds with an error message.

In case of asynchronous timestamping, all the messages (maximum limit is determined in the configuration) stored in the message log since the last periodical timestamping event are timestamped with a single (batch) timestamp. By default, the security server uses asynchronous timestamping for better performance and availability.

The security server periodically composes signed (and timestamped) documents from the message log data and archives them in the local file system. Archive files are ZIP containers containing one or more signed documents and a special linking information file for additional integrity verification purpose.

9.1 Changing the Configuration of the Message Log

Configuration parameters are defined in INI files [INI], where each section contains the parameters for a particular security server component. The default message log configuration is located in the file

```
/etc/xroad/conf.d/addons/message-log.ini
```

In order to override default values, create or edit the file

```
/etc/xroad/conf.d/local.ini
```

Create the [message-log] section (if not present) in the file. Below the start of the section, list the values of the parameters, one per line.

For example, to configure the parameters **archive-path** and **archive-max-filesize**, the following lines must be added to the configuration file:

```
[message-log]
archive-path=/my/archive/path/
archive-max-filesize=67108864
```

9.1.1 Common parameters

1. **hash-algo-id** - the hash algorithm that is used for hashing in the message log. Possible choices are **SHA-256**, **SHA-384**, **SHA-512**. Defaults to **SHA-512**.

9.1.2 Timestamping parameters

1. **timestamp-immediately** - if set to true, the timestamps are created synchronously with the message exchange, i.e., one timestamp is created for a request and another for a response. This is a security policy to guarantee the timestamp at the time of logging the message, but if the timestamping fails, the message exchange fails as well, and if load to the security server increases, then the load to the timestamping service increases as well. The value of this parameter defaults to false for better performance and availability. In case the value of the parameter is false then the timestamping is performed as a periodic background process (the time period is determined in the PlanetCross governing agency and propagated to the security servers by global configuration) and signatures stored during the time period (see parameter **timestamp-records-limit**) are timestamped in one batch.
2. **timestamp-records-limit** - maximum number of signed messages that can be timestamped in one batch. The message exchanging load (messages per minute) and the timestamping interval of the security server must be taken into account when changing the default value of this parameter. Do not modify this parameter without a good reason. Defaults to **10000**.
3. **acceptable-timestamp-failure-period** - time period in seconds, for how long the asynchronous timestamping is allowed to fail before message exchange between security servers is stopped. Set to 0 to disable this check. Defaults to **14400**.

9.1.3 Archiving parameters

1. **keep-records-for** - time in days for which to keep timestamped and archived records in the database. Defaults to **30**.
2. **archive-max-filesize** - maximum size for archived files in bytes. Reaching the maximum value triggers the file rotation. Defaults to **33554432** (32 MB).
3. **archive-interval** - time interval as Cron expression [CRON] for archiving timestamped records. Defaults to **0 0 0/6 1/1 * ? *** (fire every 6 hours).
4. **archive-path** - the directory where the timestamped log records are archived. Defaults to **/var/lib/xroad/**.
5. **clean-interval** - time interval as Cron expression [CRON] for cleaning archived records from the database. Defaults to **0 0 0/12 1/1 * ? *** (fire every 12 hours).
6. **archive-transfer-command** - the command executed after the (periodic) archiving process. This enables one to configure an external script to transfer archive files automatically from the security server. Defaults to no operation.

Depending on the load and resources of the system, it may be necessary to change the interval of the removal of old database records.

The parameter **keep-records-for-days** should be edited, for instance if the disk fills up before cleanup occurs, or alternatively, if the default period of 7 days is too short.

The parameter **clean-interval** (a Cron expression [CRON]) defines how often the system checks whether cleanup should be done. If the default period of 12 hours is too long or short it should be edited according to your needs.

9.2 Setting the message log acquisition level and size

9.2.1 Setting the message log acquisition level

The message log also includes the body part of the SOAP message by default. If there is information that should not be saved in the Security Server message log, such as personal

information in requests and responses that pass through the Security Server, you can switch between including / not including the body part in the log for each Security Server and each subsystem.

Refer to [『X-Road: System Parameters User Guide』 details.](#)

For example, to set not to retain the body part of the SOAP message, edit the **/etc/xroad/conf.d/local.ini** file and add the following:

```
[message-log]
soap-body-logging = false
```

9.2.2 Setting the message log size

The following shows an estimating for the file size required for saving the message log in the file system.

Each SOAP request contains 9.5 kB of metadata (SOAP namespace definition, header, signature). Response message contains 11.2 kB metadata.

In addition, once per minute, Security Server appends a batch timestamp and 3.6 kB / min of metadata for messages processed since the last timestamp was added. The message log capacity can be expressed as follows:

- $3.6\text{kB} + N * (21\text{kB} + R + A) = S$
- N = Request Per Minutes
- R = Payload length of Request(kB)
- A = Payload length of Response(kB)
- S = Disk usage size Per Minutes(kB / min)

9.3 Transferring the Archive Files from the Security Server

In order to save hard disk space, it is recommended to transfer archive files periodically from the security server (manually or automatically) to an external location.

Archive files (ZIP containers) are located in the directory specified by the configuration parameter **archive-path**. File names are in the format **mlog-X-Y-Z.zip**, where X is the timestamp (UTC time in the format **YYYYMMDDHHmmss**) of the first message log record, Y is the timestamp of the last message log record (records are processed in chronological order) and Z is 10 characters long alphanumeric random. An example of an archive file name is:

mlog-20150504152559-20150504152559-a7JS05XAJC.zip

The message log package provides a helper script **/usr/share/xroad/scripts/archive-http-transporter.sh** for transferring archive files. This script uses the HTTP/HTTPS protocol (the POST method, the form name is file) to transfer archive files to an archiving server.

Usage of the script:

Options	Explanation
-d, --dir DIR	Archive directory. Defaults to '/var/lib/xroad'
-r, --remove	Remove successfully transported files from the archive directory.
-k, --key KEY	Private key file name in PEM format (TLS). Defaults to '/etc/xroad/ssl/internal.key'
-c, --cert CERT	Client certificate file in PEM format (TLS). Defaults to

	'/etc/xroad/ssl/internal.crt'
-cacert FILE	CA certificate file to verify the peer (TLS). The file may contain multiple CA certificates. The certificate(s) must be in PEM format.
-h, --help	This help text.

The archive file has been successfully transferred when the archiving server returns the HTTP status code **200**.

Override the configuration parameter **archive-transfer-command** (create or edit the file **etc/xroad/conf.d/local.ini**) to set up a transferring script. For example:

```
[message-log]
archive-transfer-command=/usr/share/xroad/scripts/archive-http-transporter.
sh -r http://my-archiving-server/cgi-bin/upload
```

The message log package contains the CGI script **/usr/share/doc/xroad-addon-messagelog/archive-server/demo-upload.pl** for a demo archiving server for the purpose of testing or development.

9.4 Using a Remote Database

The message log database can be located outside of the security server. The following guide describes how to configure and populate a remote database schema for the message log. It is assumed that access to the database from the security server has been configured.

1. Create a database user at remote database host:

```
postgres@db_host:~$ createuser -P messagelog_user
Enter password for new role: <messagelog_password>
Enter it again: <messagelog_password>
```

2. Create a database owned by the message log user at remote database host:

```
postgres@db_host:~$ createdb messagelog_dbname -O messagelog_user -E UTF-8
```

3. Verify connectivity from security server to the remote database:

```
user@security_server:~$ psql -h db_host -U messagelog_user messagelog_dbname
Password for user messagelog_user: <messagelog_password>
psql (9.3.9)
SSL connection (cipher: DHE-RSA-AES256-GCM-SHA384, bits: 256)
Type "help" for help.
messagelog_dbname=>
```

4. Stop **xroad-proxy** service for reconfiguration:

```
root@security_server:~ # service xroad-proxy stop
```

5. Configure the database connection parameters to achieve encrypted connections, in **/etc/xroad/db.properties**:

```
messagelog.hibernate.jdbc.use_streams_for_binary = true
messagelog.hibernate.dialect =
ee.ria.xroad.common.db.CustomPostgreSQLDialect
messagelog.hibernate.connection.driver_class = org.postgresql.Driver
messagelog.hibernate.connection.url =
jdbc:postgresql://db_host:5432/messagelog_dbname?
ssl=true&sslfactory=org.postgresql.ssl.NonValidatingFactory
messagelog.hibernate.connection.username = messagelog_user
messagelog.hibernate.connection.password = messagelog_password
```

6. Populate database schema by reinstalling messagelog addon package and start **xroad-proxy**

■ Ubuntu

```
root@security_server:~ # apt-get install -reinstall xroad-addon-messagelog
```

■ RHEL

```
root@security_server:~ # yum reinstall xroad-addon-messagelog
```

10. Audit Log

The security server keeps an audit log. The audit log events are generated by the user interface when the user changes the system's state or configuration. The user actions are logged regardless of whether the outcome was a success or a failure. The complete list of the audit log events is described in [SPEC-AL].

Actions that change the system state or configuration but are not carried out using the user interface are not logged (for example, PlanetCross software installation and upgrade, user creation and permission granting, and changing the configuration files).

An audit log record contains

- the description of the user action,
- the date and time of the event,
- the username of the user performing the action, and
- the data related to the event.

For example, registering a new client in the security server produces the following log record:

```
2015-07-03T10:21:59+03:00 my-security-server-host INFO [X-Road Proxy UI]
2015-07-03 10:21:59+0300 - {"event":"Register client", "user":"admin1",
"data":{"clientIdentifier":{"xRoadInstance":"EE", "memberClass":"COM",
"memberCode":"member1"},"clientStatus":"registration in progress"}}
```

The event is present in JSON [JSON] format, in order to ensure machine processability. The field event represents the description of the event, the field user represents the user name of the performer, and the field data represents data related with the event. The failed action event record contains an additional field reason for the error message. For example:

```
2015-07-03T11:55:39+03:00 my-security-server-host INFO [X-Road Proxy UI]
2015-07-03 11:55:39+0300 - {"event":"Log in to token failed", "user":"admin1",
"reason":"PIN incorrect", "data":{"tokenId":"0", "tokenSerialNumber":null,
"tokenFriendlyName":"softToken-0"}}
```

By default, audit log is located in the file

/var/log/xroad/audit.log

10.1 Changing the Configuration of the Audit Log

The PlanetCross software writes the audit log to the *syslog* (*rsyslog*) using UDP interface (default port is 514). Corresponding configuration is located in the file

```
/etc/rsyslog.d/90-udp.conf
```

The audit log records are written with level INFO and facility LOCAL0. By default, log records of that level and facility are saved to the PlanetCross audit log file

```
/var/log/xroad/audit.log
```

The default behavior can be changed by editing the *rsyslog* configuration file

```
/etc/rsyslog.d/40-xroad.conf
```

Restart the *rsyslog* service to apply the changes made to the configuration file

```
$ sudo systemctl rsyslog restart
```

The audit log is rotated monthly by *logrotate*. To configure the audit log rotation, edit the *logrotate* configuration file

```
/etc/logrotate.d/xroad-proxy
```

10.2 Archiving the Audit Log

In order to save hard disk space and avoid loss of the audit log records during security server crash, it is recommended to archive the audit log files periodically to an external storage or a log server.

The PlanetCross software does not offer special tools for archiving the audit log. The *rsyslog* can be configured to redirect the audit log to an external location.

Appendix A. Subsystem Naming Convention Best Practices

To define and format the way that subsystems are named. This Naming Convention is intended as a guideline to the naming of PlanetCross subsystems.

A.1 About the subsystem

PlanetCross members must declare parts of their information system as subsystems in order for them to provide or use PlanetCross services.

Access rights are only granted to subsystems of PlanetCross members, not PlanetCross members as companies. Services provided by, as well as the access rights to, one subsystem are independent of the services provided by the member's other subsystems.

A.2 The subsystem naming guideline

Each subsystem of the same member must have its own unique name which complies with the guidelines below.

Each company defines the PlanetCross subsystem(s), taking into account the complete information system of the company. In defining PlanetCross subsystem(s), the first thing to consider is how the company could best break down and classify their information systems (which provide or use services) in terms of handling, considering the following aspects:

- Systems which operate on the same legal basis
- Systems with a same security level access
- Systems which operate on the same technical principals (e.g. are hosted externally).

Choose names which have the following characteristics:

- Readable
- Denote meaning / relevance to the services provided or used
- Concise
- Consistent
- Scalable
- Flexible
- Allow for a variable section that completes the identification (function, service, purpose, application)

A.3 Allowable characters for subsystem names

- Lowercase alphabet
- The - (dash) delimiter may be used should the need arise to separate and distinguish key elements of the subsystem name

Appendix B. Periodic backup of security server, using CRON

Security server configurations backup should be done daily using following script and cron job.

To transfer the logs automatically to different location, we will use rsync. See the manual below, to setup rsync automatic transferring.

Keep in mind to replace following strings in the manual below, according to your environment:

- [SERVER_CODE] - Replace this with your security server code (Seen in the upper left corner, when opening the security server admin web)
- [XROAD_BACKUP_STORAGE_SERVER_IP_OR_HOSTNAME] - Replace this with the IP or the hostname of the backup storage server

B.1 Backup script

To run backup script from terminal, following command should be issued as xroad user:

```
$ /usr/share/xroad/scripts/backup_xroad_proxy_configuration.sh -s  
[SERVER_CODE] -f /var/lib/xroad/backup/conf_backup_`hostname`_`date  
+Y%Y%M%d-%H%M%S`.tar
```

Output of this script will be as following:

```
...  
  
Backup file saved to  
/var/lib/xroad/backup/conf_backup_xrd-ss-01.test.avenuecross.com_20181023-1  
41110.tar
```

B.2 Setting a Cron

To run the backup periodically, it's necessary to configure Cron to do the automatic backups using the script above.

Run **crontab -e** as xroad user in terminal and then make the Cron configuration.

```
$ su - xroad  
$ crontab -e
```

Here's an example of Cron configuration to run backups:

Add this to Cron configuration:

```
0 0 * * * /usr/share/xroad/scripts/backup_xroad_proxy_configuration.sh -s
[SERVER_CODE] -f /var/lib/xroad/backup/conf_backup_`hostname`_`date
+%%Y%%m%%d-%%H%%M%%S`.tar > /dev/null 2>>
/var/log/xroad/auto_backup_warnings.log
```

This configuration will run the backup each day at 00:00 and the backup file will be stored to **/var/lib/xroad/backup**.

It will also output all the warnings to **/var/log/xroad/auto_backup_warnings.log**

B.3 RSYNC to remote backup storage server

Below are the activities that must be done in backup storage server and in security server or in all security server nodes, if clustered security server is used.

After the setup is done, you will have the backups in the backup storage server in following structure:

```
Backups
├── [SERVER_CODE]
│   ├── YEAR
│   │   ├── MONTH
│   │   │   └── HOSTNAME
│   │   │       ├── conf_backup_xrd-ss-01.test.avenuecross.com_20181023-143201.tar
│   │   │       └── conf_backup_xrd-ss-01.test.avenuecross.com_20181023-143301.tar
```

B.3.1 Backups storage server configuration

In the backup storage server, create new ssh user:

```
$ sudo adduser --system --shell /bin/bash xroad-backups
```

Create an .ssh folder and the authorized keys file:

```
$ sudo mkdir -m 750 -p /home/xroad-backups/.ssh && sudo touch
/home/xroad-backups/.ssh/authorized_keys
```

Create folder where to transfer the backup files with security server code and allow **xroad-backups** user to access it:

```
$ sudo mkdir -m 750 -p /home/xroad-backups/backups/[SERVER_CODE]/ && chown
xroad-backups -R /home/xroad-backups/
```

B.3.2 Security server configuration

NB) Following commands should be ran under root privileges.

In the security server or in all security server nodes, create an ssh key (ssh-keygen) without a passphrase for the xroad user, if one is not already existing:

```
$ su - xroad -c '/usr/bin/ssh-keygen -b 4096'
```

The key and public key will be located under folder:

```
/var/lib/xroad/.ssh/id_rsa  
/var/lib/xroad/.ssh/id_rsa.pub
```

Add the public keys to the **/home/xroad-backups/.ssh/authorized_keys** of the backups storage server machine.

From security server, accept the host key and try to connect to the backup storage server machine using ssh.

```
$ sudo ssh-keyscan -H [XROAD_BACKUP_STORAGE_SERVER_IP_OR_HOSTNAME] >  
/var/lib/xroad/.ssh/known_hosts
```

```
$ su - xroad -c "ssh  
xroad-backups@[XROAD_BACKUP_STORAGE_SERVER_IP_OR_HOSTNAME]"
```

Edit the **crontab** as xroad user in security server:

```
$ su - xroad  
$ crontab -e
```

Add the following to the **crontab** configuration:

```
10 0 * * * /usr/bin/rsync -azq --timeout=10 --remove-source-files --log-file  
'/var/log/xroad/backup-transferring.log' --include '*.tar' --exclude  
'.*'--exclude '*' --rsync-path 'mkdir -p  
/home/xroad-backups/backups/[SERVER_CODE]/`date +%Y`/`date  
+%m`/`hostname`/ && rsync' /var/lib/xroad/backup/  
xroad-backups@[XROAD_BACKUP_STORAGE_SERVER_IP_OR_HOSTNAME]:/home/xroad-back  
ups/backups/[SERVER_CODE]/`date +%Y`/`date +%m`/`hostname`/
```

Observe if any errors occur until first successful transferring in log:

```
$ tail -f /var/log/xroad/backup-transferring.log
```


Appendix C. Message logs archiving configuration

The purpose of the message log is to provide means to prove the reception of a regular request or response message to a third party. Messages exchanged between security servers are signed and encrypted. For every regular request and response, the security server produces a complete signed and timestamped document (Associated Signature Container [ASiC]).

Message log data is stored to the database of the security server during message exchange. According to the configuration, the timestamping of the signatures of the exchanged messages is either synchronous or asynchronous to the message exchange process.

The security server periodically composes signed (and timestamped) documents from the message log data and archives them in the local file system. Archive files are ZIP containers containing one or more signed documents and a special linking information file for additional integrity verification purpose.

C.1 Message logs configuration file

Configuration parameters are defined in INI files, where each section contains the parameters for a particular security server component. The default message log configuration is located in the file

```
/etc/xroad/conf.d/addons/message-log.ini
```

In order to override default values, create or edit the file

```
/etc/xroad/conf.d/local.ini
```

Create the [message-log] section (if not present) in the file. Below the start of the section, list the values of the parameters, one per line.

C.2 Parameters

The main parameters are shown below:

- **keep-records-for** - time in days for which to keep timestamped and archived records in the database. Defaults to **30**.
- **archive-max-filesize** - maximum size for archived files in bytes. Reaching the maximum value triggers the file rotation. Defaults to **33554432** (32 MB).
- **archive-interval** - time interval as Cron expression [CRON] for archiving timestamped records. Defaults to **0 0 0/6 1/1 * ? *** (fire every 6 hours).
- **archive-path** - the directory where the timestamped log records are archived. Defaults to **/var/lib/xroad/**.
- **clean-interval** - time interval as Cron expression [CRON] for cleaning archived records from the database. Defaults to **0 0 0/12 1/1 * ? *** (fire every 12 hours).
- **archive-transfer-command** - the command executed after the (periodic) archiving process. This enables one to configure an external script to transfer archive files automatically from the security server. Defaults to no operation.

C.3 Archived message logs transferring configuration

In order to save hard disk space, it is recommended to transfer archive files periodically from the security server (manually or automatically) to an external location.

To transfer the logs automatically to different location, we will use rsync. See the manual below, to setup rsync automatic transferring.

Keep in mind to replace following strings in the manual below, according to your environment:

[SS_OR_SS_CLUSTER_FQDN] - Replace this with your security server or security server cluster FQDN

[XROAD_ARCHIVE_SERVER_IP_OR_HOSTNAME] - Replace this with the IP or the hostname of the archive server

Below are the activities that must be done in archive server and in security server or in all security server nodes, if clustered security server is used.

After the setup is done, you will have the archive in the archive server in following structure (example given or single security server and clustered security server):

```
mlogs
├── [SS_FQDN]
│   ├── YEAR
│   │   └── MONTH
│   │       ├── [SS_FQDN]
│   │       │   └── mlog-20181009200637-20181009200637-qbZAuY32az.zip
│   │       │   └── ...
│   └── [SS_CLUSTER_FQDN]
│       ├── YEAR
│       │   └── MONTH
│       │       ├── [CLUSTER_NODE_1]
│       │       │   ├── mlog-20181009193003-20181009193003-475iIYTxsM.zip
│       │       │   ├── ...
│       │       └── [CLUSTER_NODE_2]
│       │           ├── mlog-20181009185003-20181009185003-kQ5FqMZWnb.zip
│       │           └── ...
└──
```

C.3.1 Archive server configuration

In the archive server, create new ssh user(xroad-archive):

```
$ sudo adduser --system --shell /bin/bash xroad-archive
```

Create an .ssh folder and the authorized keys file:

```
$ sudo mkdir -m 755 -p /home/xroad-archive/.ssh && sudo touch /home/xroad-archive/.ssh/authorized_keys
```

Create folder where to transfer the archived logs with name of the Security Server or Cluster and allow **xroad-archive** user to access it:

```
$ sudo mkdir -m 755 -p /home/xroad-archive/[SS_OR_SS_CLUSTER_FQDN]/ && chown
```

```
xroad-archive /home/xroad-archive/[SS_OR_SS_CLUSTER_FQDN]/
```

C.3.2 Security server configuration

In the security server or in all security server nodes, create an ssh key (ssh-keygen) without a passphrase for the xroad user, if one is not already existing (When clustered security server, then slave node already has ssh key. It's then necessary only to make key on the master node):

```
$ su - xroad -c '/usr/bin/ssh-keygen -b 4096'
```

The key and public key will be located under folder:

```
/var/lib/xroad/.ssh/id_rsa
/var/lib/xroad/.ssh/id_rsa.pub
```

Add the public keys to the the **/home/xroad-archive/.ssh/authorized_keys** of the archived logs machine.

From security server, connect to the archive machine using ssh and accept the host key.

```
$ su - xroad -c "ssh xroad-archive@[XROAD_ARCHIVE_SERVER_IP_OR_HOSTNAME]"
```

Edit **/etc/xroad/conf.d/local.ini** configuration file and add new parameter under **[message-log]** section:

```
[message-log]
archive-transfer-command=/usr/bin/rsync -azq
--timeout=10 --remove-source-files
--log-file '/var/log/xroad/mlog-archiving.log' --include '*.zip' --exclude
'.*' --exclude '*' --rsync-path 'mkdir -p
/home/xroad-archive/mlogs/[SS_OR_SS_CLUSTER_FQDN]/`date +%Y`/`date
+%m`/`hostname`/ && rsync' /var/lib/xroad/
xroad-archive@[XROAD_ARCHIVE_SERVER_IP_OR_HOSTNAME]:/home/xroad-archive/mlo
gs/[SS_OR_SS_CLUSTER_FQDN]/`date +%Y`/`date +%m`/`hostname`/`
```

When you customize the ``archive-transfer-command`` command, please note that the command is ran by ``xroad`` user, and check if ``xroad`` user has enough permissions to access the necessary files.

Restart **xroad-proxy** service:

```
$ sudo systemctl restart xroad-proxy
```

Observe if any errors occur until first successful transferring in log:

```
$ sudo tail -f /var/log/xroad/mlog-archiving.log
```

C.4 Recommendations for production message logs archiving

Due to high volume of messages stored in the database, it's necessary to keep message logs in the database for short time of period, since otherwise the message database will bloat remarkably. It's also important to set the interval of archiving and cleaning remarkably shorter than the default options are. If the messages are large in size, it's necessary to set maximum size of archived file to higher than the potential size of the message. Below are the default parameters that can be changed in `/etc/xroad/conf.d/local.ini` configuration file, if necessary(See "9.1 Changing the Configuration of the Message Log" for the setting method).

- `keep-records-for=0` (0 day)
- `archive-max-filesize=104857600000` (100 MB)
- `archive-interval=0 0/1 * 1/1 * ? *` (fire every 1 minutes)
- `clean-interval=0 0/5 * 1/1 * ? *` (fire every 5 minutes)

Appendix D. Setting for big query

When a large query (WSDL size of 100MB or more) is communicated with Security Server, the query size that can be processed can be expanded by combining the following settings.

D.1 Enable swap

The query size that can be processed can be expanded by enabling SWAP(OS). The following is an example of using a 1GB file as the SWAP area.

```
$ sudo swapon -show
$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            1.7G   0    1.7G   0% /dev
tmpfs           345M   36M  309M  11% /run
/dev/sda1       30G   4.0G   26G   14% /
tmpfs           1.7G   8.0K   1.7G   1% /dev/shm
tmpfs           5.0M   0    5.0M   0% /run/lock
tmpfs           1.7G   0    1.7G   0% /sys/fs/cgroup
/dev/sdb1       50G   52M   47G   1% /mnt
tmpfs           345M   0    345M   0% /run/user/115
tmpfs           345M   0    345M   0% /run/user/1000

$ sudo fallocate -l 1G /swapfile
$ sudo chmod 600 /swapfile
$ ls -l /swapfile
-rw----- 1 root root 1073741824 Mar 26 07:20 /swapfile

$ sudo mkswap /swapfile
$ sudo swapon /swapfile
$ echo '/swapfile none swap sw 0 0' | sudo tee -a /etc/fstab
$ tail -n 1 /etc/fstab
/swapfile none swap sw 0 0

$ sudo swapon -show
NAME        TYPE  SIZE USED PRIO
/swapfile  file 1024M 524K  -2
```

D.2 Change proxy Xmx

The query size that can be processed can be expanded by increasing the reserved area of the heap Xmx. For example 1536MB for Xmx:

```
$ sudo vi /etc/xroad/services/local.conf
```

Add the following to the **local.conf**. Correct the value of "-Xmx" according to your environment

```
PROXY_PARAMS=" -Xms100m -Xmx1536m -XX:MaxMetaspaceSize=80m ¥
-Djavax.net.ssl.sessionCacheSize=10000 ¥
-Dlogback.configurationFile=/etc/xroad/conf.d/proxy-logback.xml ¥
-Dxroad.proxy.clientHandlers=${CLIENT_HANDLERS#?} ¥
-Dxroad.proxy.serverServiceHandlers=${SERVICE_HANDLERS#?}"
```

After setting, Restart all Security Server services.

D.3 Turn off SOAP body logging

The query size that can be processed can be expanded by setting the message log so that the body part of SOAP is not logged. Correct the following files.

```
$ sudo vi /etc/xroad/conf.d/local.ini
```

Add the following to the **local.ini**

```
[message-log]  
soap-body-logging = false
```

After setting, Restart all Security Server services.

D.4 Raise limit for SOAP body logging

The query size that can be processed can be expanded by increasing the upper limit of the logging size of the SOAP body of the message log. Correct the following files.

```
$ sudo vi /etc/xroad/conf.d/addons/message-log.ini
```

Change the **archive-max-file-size** parameter in Byte. (default 32MB)

```
archive-max-filesize=33554432
```

After setting, Restart all Security Server services.

D.5 Combination of settings and test result

An example of a memory size of 4GB is shown below. The NO.1 setting example shows that the WSDL size can be handled up to 252MB.

NO	Settings				Input Data		Converted data
	Enable SWAP	Change Xmx	Turn off SOAP body logging	Raise limit for SOAP body logging	Number of records	Total number of records	WSDL size
1	Yes(8G)	Yes(1.5G)	Yes	Yes(256MB)	390,000	190.8 MB	252MB
2	Yes(8G)	Yes(1.5G)	-	Yes(256MB)	300,000	146.8 MB	193MB
3	Yes(8G)	Yes(1.5G)	-	-	265,000	129.6 MB	171MB

Revision History

Version	Date	Details
V1.3	11/02/2020	Publish first edition.