



# CRESTONE

SEIDOR



SEIDOR

# Introduction

This document covers installation and configuration issues in an SAP environment for the correct integration and operation of CRESTONE.

# Requirements

## SAP System Types

### General Auth

The following SAP Systems are supported:

- All SAP ABAP based systems that provide RFC connectivity are supported (all communication with SAP is performed via the RFC protocol).
- SAP ABAP Systems on any database are supported (including HANA). The database used by the SAP system is irrelevant, because the integration occurs at SAP application server level.
- SAP Releases 4.6C and newer are supported.
- All operating systems are supported.

### unsupported

- SAP systems that do not run ABAP.
- SAP systems without RFC connectivity.

## Required Ports

SAP NetWeaver component	Port
SAP Application Server	33<NN>
Message Server	36<NN>
Secure Network Communication (SNC)	48<NN>
SAP-Router	3299

For more information, see [SAP Help](#)

# SAP Authorization Objects

To use Crestone, you need an SAP connection user with the necessary authorization. Authorizations are assigned via authorization objects in SAP.

Please refer to this page to your SAP Basis administrators to obtain the corresponding authorization objects for your SAP connection user.

The authorizations in the "General Authorization Objects" section are required to establish an SAP connection to the SAP application server.

The required authorizations for each component are detailed in its corresponding section.

Crestone collected and combined the required authorizations for all components into SAP roles. You can download the SAP profiles and upload them to your SAP system:

## Supported

The following authorization objects are required to establish a connection to SAP.

S_RFC	RFC_TYPE=FUGR; RFC_NAME=SYST; ACTVT=16
S_RFC	RFC_TYPE=FUGR; RFC_NAME=SRFC; ACTVT=16
S_RFC	RFC_TYPE=FUGR; RFC_NAME=RFC1; ACTVT=16

## Report

Necessary SAP authorizations

S_RFC	RFC_TYPE=FUGR; RFC_NAME=ZXTRACTABAP; ACTVT=16
S_TABU_NAM	ACTVT=03; TABLE=TRDIR, TRDIRT, TSTC, VARID
S_GUI	ACTVT=61
S_TABU_DIS	ACTVT=03; DICBERCLS=&NC&
S_TABU_DIS	ACTVT=03; DICBERCLS=SS
S_BTCH_ADM	BTCADMIN=Y
S_BTCH_JOB	JOBGROUP=*; JOBACTION=RELE

# Download SAP profile for Report

To execute a report with Crestone, the SAP connection user needs explicit authorization to execute the report. Authorization can be granted using one of the following methods:

- [Assign the authorization object Z\\_TS\\_PROG](#)
- [Assign an authorization group](#)

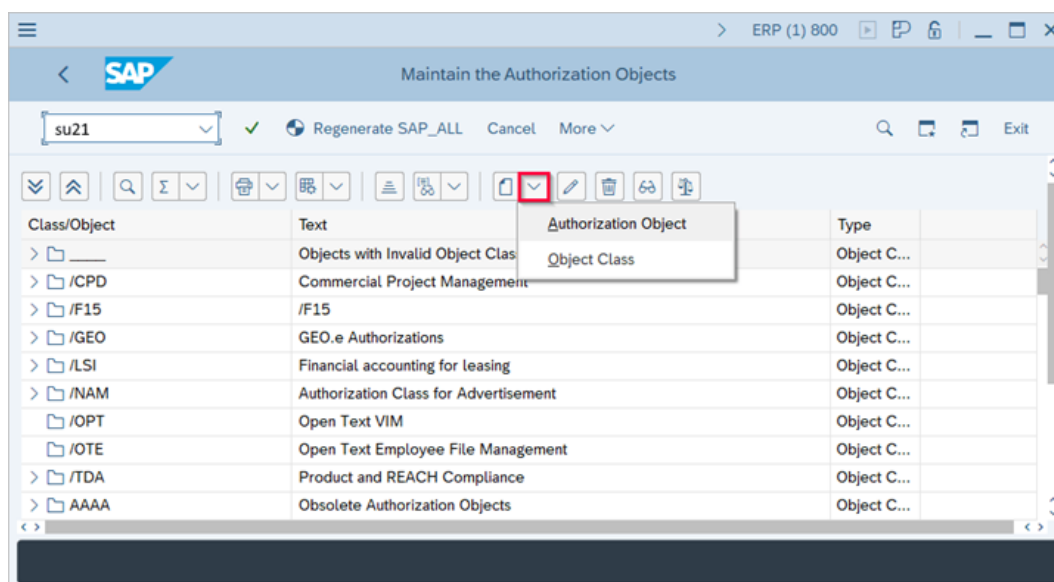
## Create the Custom Authorization Object Z\_TS\_PROG

The following article shows how to create the Z\_TS\_PROG authorization object for the custom function module Z\_CRES\_IS\_REMOTE\_REPORT.

Crestone Software custom function module **Z\_CRES\_IS\_REMOTE\_REPORT** enables the extractions of reports from SAP systems. If no authorization group is assigned to a report, Z\_CRES\_IS\_REMOTE\_REPORT uses a custom authorization object Z\_TS\_PROG to verify whether the SAP user is allowed to extract a report.

The access to reports is granted based on the name of the report.  
Create the Custom Authorization Object Z\_TS\_PROG

1. Use transaction SU21 to create a new authorization object.
2. Expand the Create menu and click [Authorization Object]. The window "Create Authorization Object" opens.



3. Enter the following values:

Object: Z\_TS\_PROG

Text: Theobald Software Report Authorization

The screenshot shows the 'Create Authorization Object' dialog box in SAP. The 'Object' field is set to 'Z\_TS\_PROG', 'Text' is 'Crestone Software', 'Class' is 'BC\_A' with 'Basis: Administration' selected, and 'Author' is 'Seidor'. The 'Authorization fields' section contains a table with one entry: 'S\_NAME' with the description 'ABAP Program Name'. Below this is a section for 'Authorization Object Documentation' with a 'Create Object Documentation' button. At the bottom, there is a 'Field maintenance' button and a status bar with a green checkmark.

Authorization Field	Short Description...
S_NAME	ABAP Program Name

4. Click [Continue] to enable editing of the section Authorization fields.

5. Manually enter S\_NAME as the first entry in Authorization fields.

6. Click [Save] to save the authorization object.

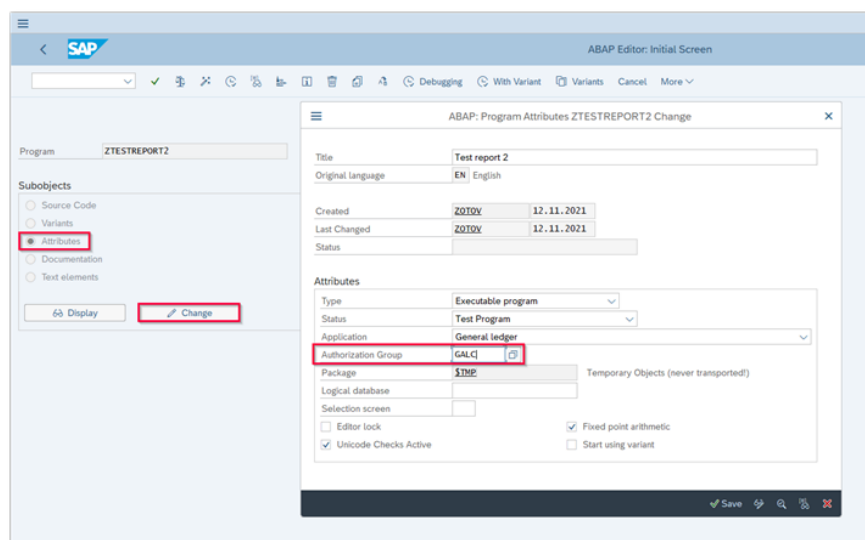
# Authorize Access to Reports via Authorization Groups

The following article shows how to set up access to reports by assigning authorization groups to reports.

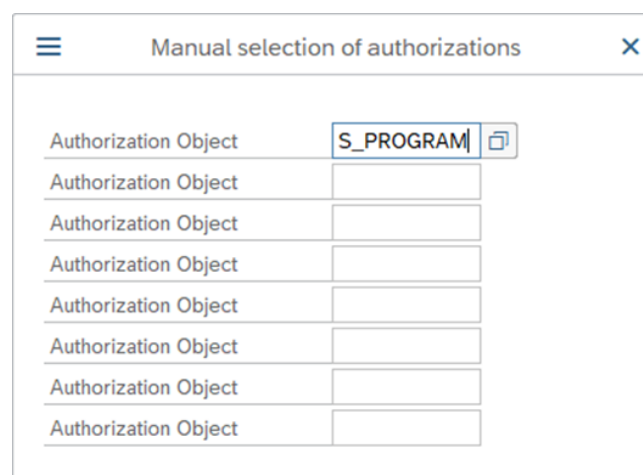
Access is then granted through the S\_PROGRAM authorization object, see: [SAP Note](#)

## Set Up Access to Specific Reports

1. Set Up Access to Specific Reports Log into SAP and use transaction code SE38 to open the ABAP Editor
2. Enter the name of the report you want to access and select Attributes as the Subobjects.
3. Click [Change]. A window that contains the program attributes opens.
4. Assign an authorization group.



5. Edit or create a user role you want to grant access to (transaction code PFCG).
6. Manually assign the authorization object S\_PROGRAM to the user role



7. Select the actions SUBMIT and BTCSUBMIT in the S\_PROGRAM object field P\_ACTION.
8. Assign the same authorization group that is assigned to the report to the S\_PROGRAM object field P\_GROUP.
9. Save and generate the authorization.
10. Assign the user role to users.



# Table

## Necessary SAP authorizations

S_RFC	ACTVT=16;
RFC_TYPE=FUGR;	
RFC_NAME=SDTX, SDIFRUNTIME,Z_CRESTONE, Z_CRESTONE_READ_TABLE	
S_TABU_DIS	ACTVT=03;
DICBERCLS=XXXX	
S_TABU_NAM	ACTVT=03;
TABLE=DD02V, DD17S, DD27S, ENLFDIR S_DSAUTH	ACTVT=16;

XXXX (stands for a placeholder) is the authorization group for the table.

To determine, which authorization group belongs to which table, check the table TDDAT – Maintenance Areas for Tables. If the table is not listed, the authorization group is &NC&. For authorizing specific tables use authorization object S\_TABU\_NAM instead of S\_TABU\_DIS.

## ODP

For a complete and detailed list of authorization objects refer to [SAP Note 2855052](#) – Authorizations required for ODP Data Replication API 2.0.

S_TABU_NAM	ACTVT=03; TABLE=TCURX
------------	-----------------------

# SAP installation and configuration

## Transport orders required for crestone's proper operation

These transport orders contain the packages necessary for the correct operation of Crestone. This is because Crestone internally executes custom RFCs.

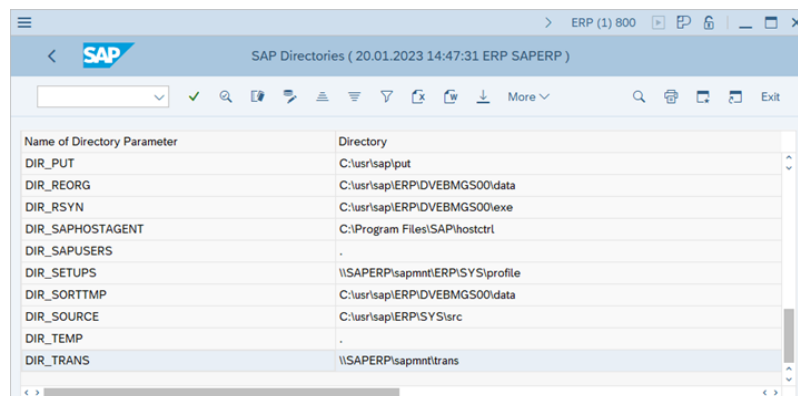
## Import an SAP Transport Request

The following article shows how to import transport requests for custom functions modules.

### Upload SAP Transport Requests to SAP

If you have access to the file system of SAP, you can copy and paste the files of your transport request directly into the data and cofiles folders of your SAP system. If you don't have access to the file system, follow the steps below to upload the files of your transport request using the SAP function module ARCHIVFILE\_CLIENT\_TO\_SERVER:

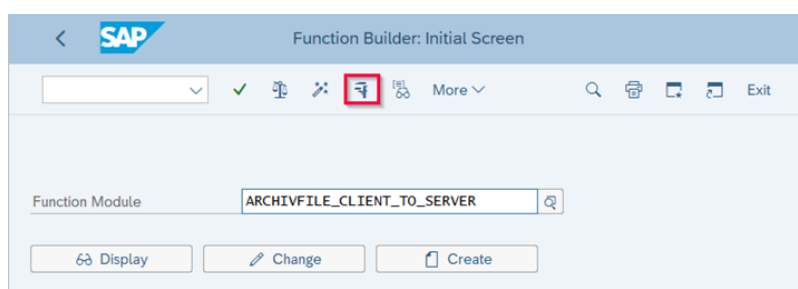
1. Unzip the transport request provided by the seidor analytics team in the installation directory of your product.
2. Open SAP and go to transaction AL11.
3. Find the entry DIR\_TRANS in the column Name of Directory Parameter. Note or copy the path shown in the column Directory.



The screenshot shows the SAP transaction AL11, titled 'SAP Directories ( 20.01.2023 14:47:31 ERP SAPERP )'. It displays a table with two columns: 'Name of Directory Parameter' and 'Directory'. The entry 'DIR\_TRANS' is highlighted, showing the directory path '\\SAPERPIsapmnttrans'.

Name of Directory Parameter	Directory
DIR_PUT	C:\usr\sap\put
DIR_REORG	C:\usr\sap\ERP\DVEBMGS00\data
DIR_RSYN	C:\usr\sap\ERP\DVEBMGS00\exe
DIR_SAPHOSTAGENT	C:\Program Files\SAP\hostctrl
DIR_SAPUSERS	.
DIR_SETUPS	\\SAPERPIsapmnt\ERP\SY\profile
DIR_SORTTMP	C:\usr\sap\ERP\DVEBMGS00\data
DIR_SOURCE	C:\usr\sap\ERP\SY\src
DIR_TEMP	.
DIR_TRANS	\\SAPERPIsapmnt\trans

4. Go to SAP transaction SE37.
5. Enter name of function module ARCHIVFILE\_CLIENT\_TO\_SERVER and click [Test/Execute].



The screenshot shows the SAP transaction SE37, titled 'Function Builder: Initial Screen'. It displays a search bar with the function module 'ARCHIVFILE\_CLIENT\_TO\_SERVER' entered. Below the search bar are buttons for 'Display', 'Change', and 'Create'.

Function Module: ARCHIVFILE\_CLIENT\_TO\_SERVER

Buttons: Display, Change, Create

6. In the field PATH you select your request file from from step 1. The name of the file starts with an "R", e.g., R900472.
7. In the field TARGET PATH you construct your target path using the following pattern:  
{copied path from step 2} \data \{request file name}.
8. Enable case-sensitivity and click [Execute]. When prompted, confirm the upload.

Test para grupo funciones	OPTA
Módulo funciones	ARCHIVFILE_CLIENT_TO_SERVER
Mayúsculas/Minúsculas	<input type="checkbox"/>

Parámetros p.import	Valor
PATH	
TARGETPATH	

9. In the field PATH you select your cofile from from step 1. The name of the file starts with a "K", e.g., K900472.
10. In the field TARGET PATH you construct your target path using the following pattern:  
{copied path from step 2} \cofiles \{cofile name}.
11. 11. Enable case-sensitivity and click [Execute]. When prompted, confirm the upload.


The files are now available in SAP.

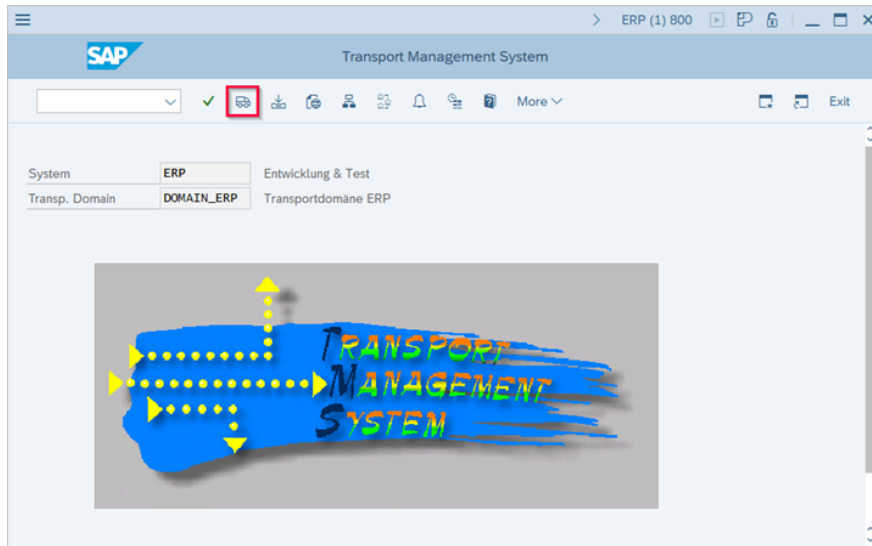
## Note

Another method for uploading files to SAP is the SAP transaction CG3Z. This transaction is only available on ERP systems.

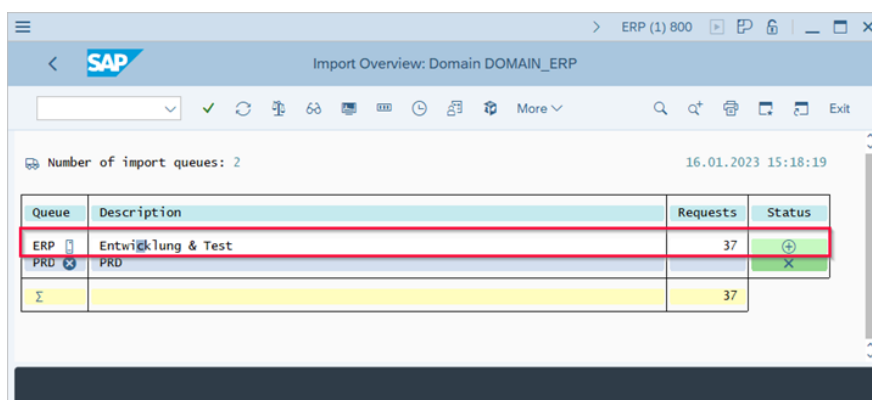
# Import SAP Transport Requests

Follow the steps below to add the transport requests to the import queue and import them:

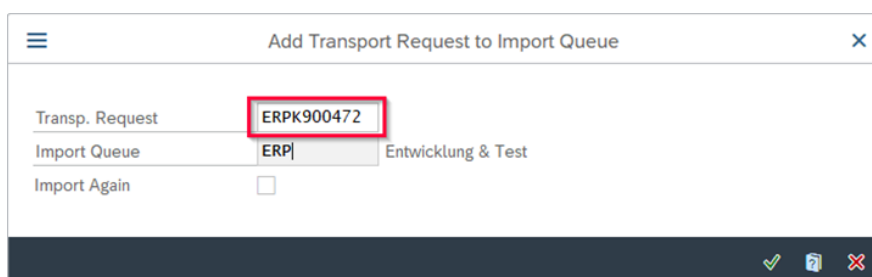
1. Go to SAP transaction STMS to open the transport management system.
2. Click [Import Overview] (  icon).



3. Double click on the import queue in which you want to load the transport request into.



4. Open the transport request selection dialog via More > Extras > Other Requests > Add.
5. Select the transport request and confirm. If prompted, confirm the import.



6. Select your transport request from the list and click [Import Request] (icon). The window "Import Transport Request" opens.
7. Enter the target client. If the version of the SAP system where the transport request was created differs from your SAP system version, select the option Ignore Invalid Component Version.

The screenshot shows the 'Import Transport Request' dialog box. The 'Options' tab is active. In the 'Import Options' section, the checkbox 'Ignore Invalid Component Version' is checked and highlighted with a red rectangle. Other options like 'Leave Transport Request in Queue for Later Import', 'Import Transport Request Again', 'Overwrite Originals', 'Overwrite Objects in Unconfirmed Repairs', 'Ignore Non-Permitted Transport Type', 'Ignore Non-Permitted Table Class', and 'Ignore Predecessor Relations' are unchecked.

8. Confirm your settings.

### The transport request is imported.

Check the Status of Transport Requests

The import overview of the transport management system (transaction STMS) lists all transport requests.

The status of the transport requests is displayed in the column "RC".

A green bar indicates that the import was successful. In case of warnings or errors, double click on the icon to view the error messages.

The screenshot shows the 'Import Queue: System ERP' table in SAP. The table has columns: Number, Request, RC, Owner, and Short Text. The row for request ERPK900472 has a green bar in the RC column, indicating a successful import.

Number	Request	RC	Owner	Short Text
36	ERPK900417		SEIDORA	report auth object transport test
37	ERPK900464		SEIDORA	CRESTONE SOFTWARE REPORT EXTRACTION FUNCTION MODULE
38	ERPK900472		SEIDORA	Z_CRES_DELETE_LOG_ENTRIES

# TCP/IP CONFIGURATION and ACL FILES files

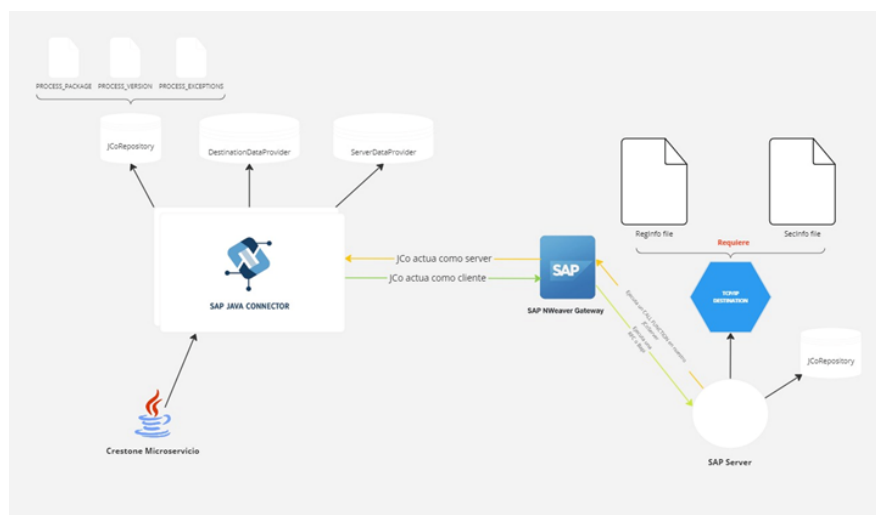
Why is this configuration required?

SAP needs to define communication destinations that allow integration with external systems, such as our microservice Crestone, developed in Java and using SAP JCo. The TCP/IP Destination configuration in transaction SM59 is essential because:

- SAP cannot communicate with external applications without an explicit target definition.
- Allows Crestone Microservice to register with SAP as a valid point of communication.
- Establishes a secure and authenticated channel for the execution of RFC (Remote Function Call) functions.

SAP requires the implementation of access control files (ACL) that regulate which programs can register and run in SAP Gateway, that is why we must configure the RegInfo and SecInfo files to enable the registration of the CRESTONE\_SERVER programID.

The configuration of TCP/IP Destination in SAP together with the correct management of the access control files (Reginfo and Secinfo) in SAP Gateway is essential for



# How to configure it?

## Connection Creation TCP/IP

1. Access the SM59 transaction.
2. Create a new TCP/IP type connection.
3. In the 'Destination name' field, enter: CRESTONE\_SERVER.



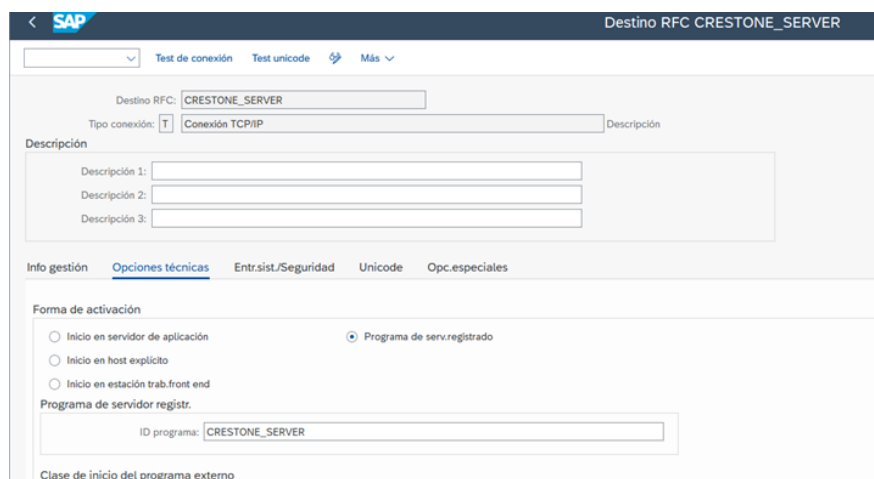
Crear destino

Destino: \* CRESTONE\_SERVER

Tipo de conexión: \* T Conexión RFC con el programa externo medi...

✓ ✗

4. Select the 'Connection Type' as TCP/IP.
5. Set the gateway host and TCP service to sapgw00.



Destino RFC CRESTONE\_SERVER

Test de conexión Test unicode Más

Destino RFC: CRESTONE\_SERVER

Tipo conexión: T Conexión TCP/IP Descripción

Descripción

Descripción 1:

Descripción 2:

Descripción 3:

Info gestión Opciones técnicas Entr.sist./Seguridad Unicode Opc.especiales

Forma de activación

☐ Inicio en servidor de aplicación ☒ Programa de serv.registrado

☐ Inicio en host explícito

☐ Inicio en estación trab.front end

Programa de servidor registr.

ID programa: CRESTONE\_SERVER

Clase de inicio del programa externo

# Configuration in SAP

## Connection Creation TCP/IP

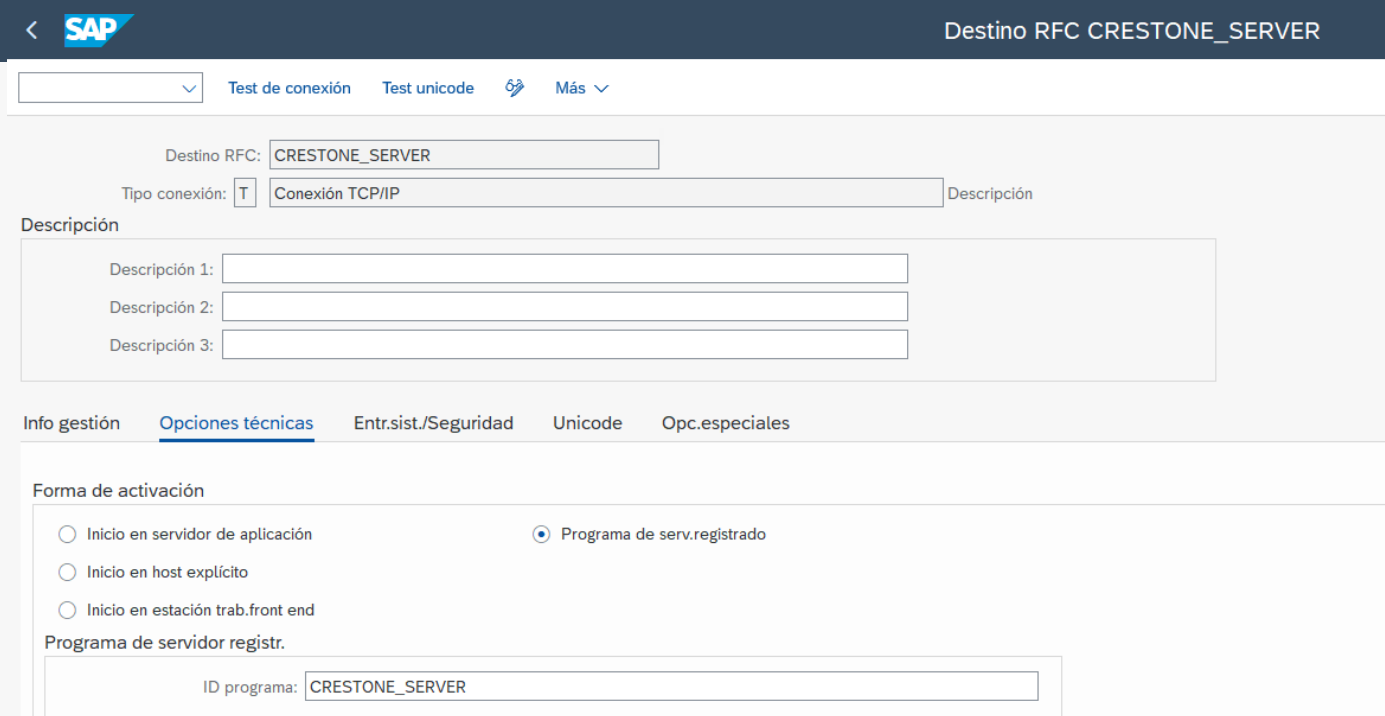
To enable communication between SAP and the crestone, a TCP/IP connection must be configured in SAP using transaction SM59.

### Steps

1. Access the SM59 transaction.
2. Create a new TCP/IP type connection.
3. In the 'Destination name' field, enter: CRESTONE\_SERVER.



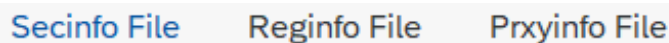
4. Select the 'Connection Type' as TCP/IP.
5. Set the gateway host and TCP service to sapgw00.







To enable the CRESTONE\_SERVER program to communicate with SAP, it is necessary to configure access in SAP Gateway using transaction SMGW.

1. Access the SMGW transaction.




### 3. Add the standard in secinfo file and define the following parameters:


 Create Line in Secinfo File 

P/D (\*):


TP (\*):

USER (\*):



HOST (\*):  

USER-HOST:  

Comment:


 Save


### 4. Add the other standard in Reginfo file


 Create Line in Reginfo File 

P/D (\*):

TP (\*):


HOST:  

ACCESS:  

Cancel:  

NO:

Comment:

 Save



© 2024 Seidor o una empresa filial de Seidor. Todos los derechos reservados.

Ninguna parte de esta publicación puede ser reproducida o transmitida en ninguna forma

o para cualquier propósito sin el permiso expreso de Seidor o de una empresa afiliada a Seidor. La información aquí contenida puede ser modificada sin previo aviso.

Algunos productos de software comercializados por Seidor y sus distribuidores contienen componentes de software propietarios de otros proveedores de software. Las especificaciones de los productos nacionales pueden variar.

Estos materiales son proporcionados por Seidor o una compañía afiliada de Seidor para fines informativos únicamente, sin representación ni garantía de ningún tipo y Seidor o sus empresas afiliadas no serán responsables de los errores u omisiones con respecto a los materiales. Las únicas garantías de los productos y servicios de Seidor o de sus empresas afiliadas son las que se establecen en las declaraciones de garantía expresas que acompañan a dichos productos y servicios, en su caso. Nada de lo aquí expuesto debe interpretarse como constitutivo de una garantía adicional.

Seidor y otros productos y servicios de Seidor mencionados en el presente documento, así como sus respectivos logotipos son marcas comerciales o marcas registradas de Seidor (o una empresa filial de Seidor) en España y otros países. Todos los otros nombres de productos y servicios mencionados son marcas comerciales de sus respectivas empresas.