X.509 Certificate Logon over the ITS

Security

Version 1.0: English
March 31, 1999
Copyright

©Copyright 1999 SAP AG. All rights reserved.

No part of this documentation may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG.

SAP AG further does not warrant the accuracy or completeness of the information, text, graphics, links or other items contained within these materials. SAP AG shall not be liable for any special, indirect, incidental, or consequential damages, including without limitation, lost revenues or lost profits, which may result from the use of these materials. The information in this documentation is subject to change without notice and does not represent a commitment on the part of SAP AG in the future.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft®, WINDOWS®, NT® and EXCEL® and SQL-Server® are registered trademarks of Microsoft Corporation.

IBM®, OS/2®, DB2/6000®, AIX®, OS/400® and AS/400® are a registered trademark of IBM Corporation.

OSF/Motif® is a registered trademark of Open Software Foundation.

ORACLE® is a registered trademark of ORACLE Corporation, California, USA.

INFORMIX®-OnLine for SAP is a registered trademark of Informix Software Incorporated.

UNIX® and X/Open® are registered trademarks of SCO Santa Cruz Operation.

ADABAS® is a registered trademark of Software AG.

SECUDE® is a registered trademark of GMD-German National Research Center for Information Technology.

SAP®, R/2®, R/3®, RIVA®, ABAP®, SAPoffice®, SAPmail®, SAPaccess®, SAP-EDI®, SAP ArchiveLink®, SAP EarlyWatch®, SAP Business Workflow®, R/3 Retail® are registered trademarks of SAP AG.

SAP AG assumes no responsibility for errors or omissions in these materials.

All rights reserved.
Contents

INTRODUCTION .................................................................................................................................................... 1

PREREQUISITES FOR USING THIS DOCUMENT ................................................................................................ 2
Terminology and Abbreviations .......................................................................................................................... 2
Reference Material ........................................................................................................................................... 3

LOGON TO THE R/3 SYSTEM USING CLIENT CERTIFICATES .............................................................................. 4

PREREQUISITES ................................................................................................................................................. 4
PROCESS FLOW ................................................................................................................................................ 6
RESULT ............................................................................................................................................................. 6

ADMINISTRATION TASKS .................................................................................................................................. 7

CONFIGURING THE WEB SERVER .................................................................................................................. 7
CONFIGURING THE ITS COMPONENTS ........................................................................................................... 8
Prerequisites ...................................................................................................................................................... 8
Procedure .......................................................................................................................................................... 8
Result ............................................................................................................................................................... 10

CONFIGURING THE R/3 SYSTEM’S APPLICATION SERVER ............................................................................. 11
Prerequisites ...................................................................................................................................................... 11
Procedure .......................................................................................................................................................... 11
Result ............................................................................................................................................................... 12

MAINTAINING THE USER’S EXTERNAL IDENTIFICATION IN THE R/3 SYSTEM ...................................................... 13
Prerequisites ...................................................................................................................................................... 13
Procedure .......................................................................................................................................................... 13
Typographical Information

The following table explains the meanings of the various formats, symbols, and standard notations used in this document.

<table>
<thead>
<tr>
<th>This text format</th>
<th>helps you identify</th>
</tr>
</thead>
<tbody>
<tr>
<td>Screen Text</td>
<td>words or characters you see on the screen (this includes system messages, field names, screen titles, menu names, and menu items).</td>
</tr>
<tr>
<td>User Entry</td>
<td>exact user input. These are words and characters you type on the keyboard exactly as they are in the documentation.</td>
</tr>
<tr>
<td>&lt;Variable User Entry&gt;</td>
<td>variable user input. Pointed brackets indicate that you replace these variables with appropriate keyboard entries.</td>
</tr>
<tr>
<td>ALL CAPITALS</td>
<td>report names, program names, transaction codes, table names, ABAP language elements, file names, and directories.</td>
</tr>
<tr>
<td>Book Title</td>
<td>cross-references to other books or references.</td>
</tr>
<tr>
<td>KEY name</td>
<td>keys on your keyboard. Most often, function keys (for example, F2 and the ENTER key) are represented this way.</td>
</tr>
<tr>
<td>Technical Object Name</td>
<td>names of technical objects outside of the R/3 System (for example, UNIX or Windows NT filenames or environment variables).</td>
</tr>
</tbody>
</table>

This icon helps you identify

- **Example**
  - an Example. Examples help clarify complicated concepts or activities.

- **Note**
  - a Note. Notes can contain important information like special considerations or exceptions.

- **Caution**
  - a Caution. Cautions help you avoid errors such as those that could lead to data loss.
Introduction

In Release 3.0D, we introduced the R/3 Internet Application Components (IACs) to enable you to offer certain business scenarios to Internet (or Intranet) users. By implementing IACs, users can access your R/3 System from the Internet or Intranet to perform business to business, customer to business, or company-internal processes. For example, you can publish an online company product catalog or create an employment opportunities site.

Internet Transaction Server

To integrate the R/3 System with the Internet, we have implemented the SAP Internet Transaction Server (ITS). The ITS allows you to perform your tasks in the R/3 System using a Web browser as the user interface. It controls the communications and makes the necessary data format conversions between the Web server and the R/3 System.

User Context

To establish the context under which the IAC should run, each Internet application has its own service file. The service file contains information such as the hostname of the application server, the client in the R/3 System, or the language. You can also use a global service file to specify default information for all of your IACs. Entries in an application-specific service file override those in the global service file.

The IAC also establishes the user context depending on entries in the service file. There are two main scenarios:

- Service User Scenario
  The IAC establishes a service user if there are user and password entries in either of the service files. The service user must have a user master record and authorizations in the corresponding R/3 System. Internet users who call the IAC log on to the R/3 System under the service user and work in the R/3 System using its authorizations.

- Named User Scenario
  If no user and password entries exist in either of the service files, then the IAC requests the logon information from the user in an HTML logon screen. The user logs on to the R/3 System by providing his or her user-id and password. The user session runs under his or her user account in the R/3 System and he or she must have the appropriate authorizations to be able to process the IAC.

  Note

  The application decides which scenario it uses! An application designed for service users cannot use named users.

Client Certificate Authentication for Named Users

It is becoming increasingly more popular for Internet users to authenticate themselves on Web servers using client certificates, and as of Release 4.5B, we further integrate the R/3 System into the Internet world by supporting the use of this common practice. When accessing R/3 Internet applications that require named users, Internet users who have authenticated themselves on the Web server using their client certificates can also log on to the corresponding R/3 System over the ITS without having to provide further authentication. As with the standard named-user scenario, the user session runs under the user-id of the certificate owner and not under a service user.
Prerequisites for Using this Document

This document describes how you can set up your R/3 System and the ITS to accept X.509 client certificates for user authentication. It describes the logon process and the administration measures that are necessary to support it. To effectively use this document, you should be familiar with R/3 System’s user and system administration, as well as the ITS architecture and administration.

Terminology and Abbreviations

You should be familiar with the following terms and abbreviations:

- **HyperText Transfer Protocol (HTTP)**
  Application-level protocol used in Internet communications. The HyperText Transfer Protocol controls the communication between the Web browser (HTTP client) and the Web server (HTTP server).

- **Secure Sockets Layer (SSL) protocol**
  Protocol that uses strong authentication mechanisms and encryption to secure data being transferred over the Internet.

- **HTTPS**
  HTTP over SSL. Data packets transferred across a HTTPS connection are encrypted with SSL. When using HTTPS, you also have the option of requiring strong authentication for both the client and the server sides of a HTTP connection.

- **Client certificates / X.509 client certificate**
  A digital document that contains the information necessary to prove a user’s identity as well as for encrypting and decrypting messages. The most widely used format for client certificates is the X.509 standard.

- **Certification Authority (CA)**
  A third-party instance that issues certificates. The CA’s role is to guarantee the identity of the owner of a certificate.

- **Internet Application Component (IAC)**
  Complete business solution for linking R/3 Systems to the Internet. Internet Application Components allow you to run your company’s business processes from the Internet (or within your Intranet). Internet users execute their tasks in the R/3 System using a Web browser as their user interface.

- **Internet Transaction Server (ITS)**
  Interface between the R/3 Systems and the Internet. When an Internet user starts an Internet Application Component (IAC) from a Web browser, the request is passed to the HTTP server. The HTTP server transmits the request to the Internet Transaction Server (ITS), which sets up a connection to the R/3 System. Once a connection has been established, the ITS controls the communication and the data exchange between the R/3 System and the HTTP server. The ITS consists of several components to include the WGate, the AGate, and the ITS Manager.
• **WGate**
  ITS component located on the Web server. The WGate controls the communication between the Web server and the AGate component of the ITS. Because the Web browser \(\leftrightarrow\) Web server communication uses the HTTP(S) protocol, and the WGate \(\leftrightarrow\) AGate communication uses SAP-defined protocols, the WGate is needed to make the protocol conversions necessary for successful communication.

• **AGate**
  ITS component located on the main ITS server. The AGate controls the communication to and from the R/3 System application server. It receives the data from the WGate and converts it to the SAP DIAG protocol or RFC, and vice versa. It also handles the logon process to the R/3 System application server.

• **ITS Manager**
  A unit similar to the message server in a R/3 System. It manages the AGates and their current workload for load balancing. For example, it starts new AGates if the load requirements demand it, or it restarts an AGate that terminated unexpectedly.

• **Secure Network Communications (SNC)**
  Software layer in R/3 Systems that enable the R/3 Systems to communicate with an external security product. The external product can protect the communication links between the components of the R/3 System. In addition, you can use features provided by the security product to complement and enhance the standard functions already provided by the R/3 System. For example, you can apply encryption to the data communications between the R/3 System and the ITS components.

**Reference Material**

You should also have the following documentation available for further reference:

**Note**

Use the following links to access SAPNet:

- [http://sapnet.sap-ag.de](http://sapnet.sap-ag.de) (Germany)
- [http://sapnet.sap.com](http://sapnet.sap.com) (Other countries)

• **SNC User's Guide, Version 1.2**
  The SNC User's Guide is available in SAPNet. Use the alias 'systemmanagement' and then choose Media Center \(\rightarrow\) Literature (for example, see [http://sapnet.sap.com/systemmanagement](http://sapnet.sap.com/systemmanagement)).

• **SAP@Web Installation Guide, Releases 3.0D to 4.5B, Material Number: 51006024**
  The SAP@Web Installation Guide is also available in SAPNet. See the alias 'instguides' and then choose the appropriate release.

• **R/3 Security Guide VOLUME II: R/3 Security Services in Detail, Chapter 2-3: Network Infrastructure and Chapter 2-10: Special Topics**
  The R/3 Security Guide is available in SAPNet. See the alias 'securityguide'.

• Documentation on your Web server.
• Documentation for the security product that you use for SNC.
Logon to the R/3 System using Client Certificates

User logons to the R/3 System over the ITS using client certificates is a new usability and security feature for the R/3 Internet Application Components (IACs). Internet users who possess valid client certificates and authenticate themselves on the Web server (using SSL) can access R/3 IACs over the ITS without having to provide further authentication. This feature is available for those IACs that use named users in the R/3 System instead of the service user scenario.

**Prerequisites**

There are several administration tasks that you need to perform before being able to use client certificate logons over the ITS. Figure 1 shows the elements and components that are involved in each of these tasks. A description of each task follows.

![Figure 1: Prerequisites for using Client Certificates over the ITS](image)

You need to enable HTTPS connections on the Web server and configure it to authenticate users' client certificates. See the section titled *Configuring the Web Server* and your Web server documentation for more information.

**Note**

When using client certificates for logon to the R/3 System, the user authentication process occurs on the Web server! The Internet user's authentication in the R/3 System is based on a trust relationship. The R/3 System itself does not additionally verify the client certificate; it trusts that the Web server has authenticated the user! Therefore, it is very important to configure your Web server correctly!
You need to install the ITS version 2.2 or higher.

We do not describe the ITS installation process in this document. Refer to the SAP@Web Installation Guide for more information.

**Note**

We also highly recommend that you protect the ITS network by using firewalls and SAProuters. We do not describe the corresponding administration measures in this document. Refer to the R/3 Security Guide VOLUME II: R/3 Security Services in Detail, Chapter 3: Network Infrastructure and Chapter 10: Special Topics → Protecting R/3 Internet Application Components for a description on how to configure your firewalls and SAProuters.

You need to use Secure Network Communications (SNC) to guarantee secure communications (to include authentication) between the WGate and the R/3 System.

SNC requires the use of an external security product to provide its protection. There are three levels of protection that are available with SNC: authentication, integrity, and privacy protection. To receive authentication, integrity and privacy protection, you need to use a security product that has been certified by the SAP Complementary Software Program (CSP™). For authentication only, you can also use the Microsoft® NT LAN Manager Security Support Provider (NTLMSSP) provided by SAP.

**Note**

The Microsoft® NTLMSSP is available for Windows NT environments only and its protection is limited to authentication. If you use it as the security provider, then you do not have any integrity or privacy protection for the communication between the WGate and the R/3 System. Because user authentication in the R/3 System in this scenario is based on a trust relationship, we recommend also protecting the communications from manipulation, which requires the complete SNC solution. A certified security product can guarantee not only the user’s authentication; it can also guarantee the integrity of the client certificate once it has reached the R/3 System.

You can find information on both scenarios, as well as a complete description on activating and configuring SNC, in the SNC User’s Guide. For configuration information specific to the client certificate logon scenario, see the sections in this document Configuring the ITS Components and Configuring the R/3 System’s Application Server.

You need to configure the R/3 System and the ITS for using client certificates. See the sections Configuring the ITS Components and Configuring the R/3 System’s Application Server for details on the configuration.

You need to enter the external identifications for the users who use client certificates in the R/3 System. See the section titled Maintaining the User’s External Identification in the R/3 System for details.
Logon to the R/3 System using Client Certificates

Process Flow

Figure 2 shows an overview of the logon process using client certificates over the ITS.

1. The Internet user authenticates him or herself on the Web server using his or her client certificate (using SSL).
2. He or she then accesses an IAC transaction.
3. If the user's authentication on the Web server was successful, the ITS WGate passes the user's client certificate from the Web server to the AGate.
4. The AGate establishes the connection to the R/3 System's application server and passes the client certificate on to the R/3 System.
5. If the R/3 System can uniquely identify the owner of the client certificate as a user in the R/3 System, then it logs the user on under the R/3 System user-id and continues processing the IAC. If not, then:
   - If the logon is a dialog connection, and certain information cannot be resolved (for example, if the R/3 System client is not available, or if the certificate belongs to more than one user in the R/3 System), then the user is prompted for the information.
   - If the logon occurs using RFC, and the client or user cannot be determined, then the connection terminates with an error.

Result

The Internet user is logged on to the R/3 System under his or her user-id, without having to provide further authentication.
Administration Tasks

You need to perform the following administration tasks to enable SNC and the use of X.509 client certificates for logging on to the R/3 System over the ITS:

- Configuring the Web Server
- Configuring the ITS Components
- Configuring the R/3 System's Application server
- Maintaining the User's External Identification in the R/3 System

We describe these tasks in the following sections.

Configuring the Web Server

1. Enable HTTPS on the Web server and configure it to accept certificates that you trust.

   The exact procedure for this step depends on your Web server and the operating system that you use. Refer to the documentation provided by your vendor for more information.

   **Note**

   This step is very important! When Internet users use client certificates for logging on to the R/3 System over the ITS, they are not further authenticated in the R/3 System! R/3 makes sure that the user has an account, but it trusts that the Web server has authenticated the user and accepts the client certificate without performing any further verification.

   In addition, the R/3 System does not verify the issuer of the certificate. If a user possesses more than one certificate that are issued from different Certification Authorities (CAs), but contain the same identification, then the R/3 System does not detect a difference between the certificates.

   Therefore, we recommend that you take special care when configuring your Web server. For example, you could establish your own CA and configure your Web server to only accept certificates that you have issued.

2. Configure your Web server to pass the certificate on to the WGate.

   This step also depends on the Web server and the operating system that you use. Again, refer to your Web server documentation for more information.
Configuring the ITS Components

Prerequisites

The following are the prerequisites for configuring the ITS components:

- The ITS components have been installed. See the SAP@Web Installation Guide.
- The security product for using SNC has been installed on the AGate and WGate servers. See the product's documentation for more information.
- You need to know the SNC names for the AGate and the WGate and the locations of the security libraries on each of their hosts. You also need to know the SNC name of the R/3 System's application server.
- Any other product-specific tasks have been completed. For example, you may have to create security environments and distribute certificates for each component. Again, refer to the product's documentation for more details.

Procedure

1. Make the following entries in each of the component's configuration:

<table>
<thead>
<tr>
<th>Parameter / Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>2: Use NISNC based connection (SAP protocol NI plus SNC)</td>
</tr>
<tr>
<td>SncNameAGate</td>
<td>SNC name of the AGate and the ITS Manager</td>
</tr>
<tr>
<td>SncNameWGate</td>
<td>SNC name of the WGate</td>
</tr>
</tbody>
</table>

Depending on your environment, you can make the entries with the following methods:

- If you use the ITS Administration Tool, then make the entries under Security → Network Security.
- Otherwise, make the entries in the registry key
  `KEY_LOCAL_MACHINE\Software\SAP\ITS\2.0\<virtual ITS>\Connects`

Note

The AGate and the ITS Manager share the same security environment and SNC name.

2. Make sure that the path and filename of the security product's library is specified in the environment variable `SNC_LIB` on both the AGate and WGate hosts.
3. Establish the security environment for each of the components.

This step is product-specific and you need to refer to the security product's documentation. For example, you may have to create and establish security environments for each of the components. The component may then need to logon to the security product under the secure environment.

**Note**

The R/3 System needs to be able to differentiate between the two components' security environments. Therefore, if you install the AGate and the WGate on the same host, then you cannot use a global environment variable or registry key to specify the locations of each component's security environments.

In this case, use the following process-specific registry keys to specify different security environment locations or other variable values for each component.

```
HKEY_LOCAL_MACHINE\Software\SAP\ITS\2.0\<virtual ITS>\Programs\[AGate|MManager|WGate]\environment\<variable>
```

4. For each of the IAC transactions that support client certificate logons, enter the following parameters in the corresponding service file on the AGate server:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>~clientCert</td>
<td>1</td>
<td>Allow X.509 client certificates for the IAC.</td>
</tr>
<tr>
<td>~sncNameAGate</td>
<td>SNC name of the AGate</td>
<td>Optional. However, you must specify the SNC name of the AGate in one of the following ways:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Registry entry Use the same SNC name for the AGate as with the WGate ↔ AGate connection.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Entry in the global service file Specify a default SNC name for the AGate for all services that may differ from that in the WGate ↔ AGate connection.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Entry in the local service file Specify a service-specific SNC name for the AGate.</td>
</tr>
<tr>
<td>~sncNameR3</td>
<td>SNC name of the application server</td>
<td>The entry is mandatory either in the local service file or in the global service file global.srvc. An entry in global.srvc specifies a default application server SNC name for all services. An entry in a local service file overrides that in global.srvc.</td>
</tr>
<tr>
<td>~sncQoPR3</td>
<td>Quality of protection level to use for the communication</td>
<td>Possible values: 1: authentication only 2: data integrity protection 3: data privacy protection 9: use the value from the application server's profile parameter snc/data_protection_max</td>
</tr>
</tbody>
</table>
5. Restart the Web server and the ITS Manager.

**Note**

The SNC installation process also produces trace files for evaluation purposes. The ITS trace files are WGate.trc, AGate.trc, and Mmanager.trc. After installing SNC on the ITS, you should check these files for errors. If the SNC installation was successfully completed, then each of the files should contain an entry similar to the following example. (Note that some of the information is product-specific, and your entries may contain different information depending on the product that you use.)

**Example**

Trace File Entries after Successful SNC Installation

```
Fri Aug 08 13:36:17 1997
SncInit(): Trying environment variable SNC_LIB as a
gssapi library name: "c:\program files\secude\secude.dll"
File "c:\program files\secude\secude.dll" dynamically loaded as GSS-API v2
library.
The internal Adapter for the loaded GSS-API mechanism identifies as:
Internal SNC-Adapter (Rev 1.0) to SECUDE 5/GSS-API v2
```

**Result**

The ITS components can now communicate with each other and with the R/3 System using SNC (provided that SNC is also activated on the R/3 System's application server). The ITS is also capable of passing X.509 client certificates on to the R/3 System.
Configuring the R/3 System's Application Server

Prerequisites

You have installed the security product on the application server.

You also need to know the AGate's SNC name.

**Note**

To find complete information on activating and configuring SNC in your R/3 System, refer to the *SNC User's Guide*. In this section, we include only the information that is relevant to the ITS communications.

Procedure

1. Activate SNC on the application server by setting the following profile parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>snc/enable</td>
<td>1</td>
<td>Activate SNC on the application server.</td>
</tr>
<tr>
<td>snc/gssapi_lib</td>
<td>path and filename of the security library</td>
<td>determined when installing the security product</td>
</tr>
<tr>
<td>snc/identity/as</td>
<td>SNC name of the application server</td>
<td>determined when installing the security product</td>
</tr>
<tr>
<td>snc/data_protection_max</td>
<td>Maximum level of protection to use</td>
<td>Possible values: 1: authentication only 2: data integrity protection 3: data privacy protection</td>
</tr>
<tr>
<td>snc/data_protection_min</td>
<td>Minimum required data protection level</td>
<td>Possible values: 1: authentication only 2: data integrity protection 3: data privacy protection</td>
</tr>
<tr>
<td>snc/data_protection_use</td>
<td>Default level of data protection to use</td>
<td>Possible values: 1: authentication only 2: data integrity protection 3: data privacy protection 9: use the value from snc/data_protection_max</td>
</tr>
</tbody>
</table>
2. Configure the R/3 System for accepting X.509 client certificates by setting the following profile parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>snc/extid_login_diag</td>
<td>1</td>
</tr>
<tr>
<td>snc/extid_login_rfc</td>
<td>1</td>
</tr>
</tbody>
</table>


   a. Enter the System-ID and the SNC name for the AGate.

      The System-ID field is optional. The R/3 System does not need it to identify the AGate; it uses the SNC name. However, you can assign a System-ID to the AGate to improve transparency.

   b. Activate the following options:

      - Entry for RFC activated
      - Entry for diag activated
      - Entry for certificate activated

Result

The R/3 System and the AGate can now communicate using SNC protection. The R/3 System is also capable of accepting X.509 client certificates.
Maintaining the User's External Identification in the R/3 System

The R/3 System must be able to identify the owner of the certificate. Therefore, you need to enter an external identification for each user who uses a client certificate to log on to the R/3 System. The information is stored in the table USREXTID. When the R/3 System receives a client certificate, it searches the table for a corresponding user-id.

Prerequisites

You need to know the SNC names of the users who will use client certificates to log on to the R/3 System over the ITS.

Procedure

1. In Customizing for System administration, maintain the user's external identification by choosing Management of External Security Systems → External identification → Maintain external identification for the user (All types) (table USREXTID).

   The Determine Work Area: Entry dialog box appears.

2. Enter DN in the Type of external ID field.

   The Change View "Assign external ID to users": Overview screen appears with a list of existing entries. If only one entry exists, then the Overview screen is skipped and the Details screen appears for the single entry.

3. To create an entry, choose Edit → New entries. (To modify an existing entry, select the entry and choose Goto → Detail. Note that not all fields are modifiable.)

4. Enter the following information in the appropriate fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extern.ID</td>
<td>Distinguished Name as found in the user's certificate.</td>
</tr>
<tr>
<td>Serial no.</td>
<td>Serial number of the certificate; 000 is the default value.</td>
</tr>
<tr>
<td>User</td>
<td>User-id in the R/3 System.</td>
</tr>
<tr>
<td>Min. date</td>
<td>Earliest date on which the certificate is valid for logging on to the R/3 System.</td>
</tr>
</tbody>
</table>

5. Set the Activated indicator.

6. Save the data.