ITS User Management

Release 4.6C

SAP™

Copyright

Icons

Icon	Meaning
⚠	Caution
	Example
➡	Note
	Recommendation
	Syntax
	Tip

Contents

ITS User Management

ITS User Management

When implementing Internet Application Components (IACs) that enable Internet users to access business transactions in R/3, you need to be aware how the ITS behaves when a user tries to access the R/3 System from the Internet. User management is very important in this context, because it raises important security considerations for R/3 data.

For further information, see:

Logon Administration

When users access the R/3 System via the SAPgui, they have to enter valid logon information such as client, user name, password, and language. Their user authorizations in R/3 determine what they can or cannot do.

When users access the R/3 System from the Internet by starting a service to run an Internet Application Component (IAC), they may have to enter similar logon information. What they are allowed to do again depends on their user authorizations in R/3.

Logon behavior at service startup is controlled by parameter values that can be predefined in either or both of the following ITS service files:

- The service file `<service name>.srvc` for the current service

  This service file contains settings for the current service only.

- The global service file `global.srvc`

  This service file contains settings that serve as default values for all services.

The logon-related parameters you can define in these service files are listed in the following table:

Logon-Related Service Parameters

Parameter Name	Meaning	Example
`~client`	Client	000
`~login`	User name	davey
`~password`	Password	******** (encrypted password)
`~language`	Language	en

On service startup, the ITS gathers all the values required to run the service by merging the parameters defined in the service file for the current service with the parameters defined in the global service file.

Getting access to the R/3 System depends on:

- Establishing a connection
- Supplying valid logon information

Establishing a Connection

In ITS versions prior to 2.2, a connection to the R/3 System was not established until the logon information such as client, user name, password, and language was known. The functions on the R/3 logon screens were not supported.

From ITS 2.2, a connection to the R/3 System is established as soon as all the technical system parameters are known. Consequently, when the logon screen is displayed in the user's Web browser, the ITS has already established a connection to the R/3 System.

Logon Administration

This means that the HTML logon page (`login.html`) is now a regular HTML template that can send any OK code to R/3. As a result, users are able to change their passwords interactively.

Supplying Valid Logon Information

Before users can access R/3, valid logon information must be supplied either in the service files or by the user interactively.

The following conditions apply:

- If all of the logon-related parameters contain values (in **either** the service file for the current service **or** the global service file), the user does not need to provide any logon information. In this case, the ITS does not send a logon page, and the user gets direct access to R/3.

- If **neither** the service file for the current service **nor** the global service file contains a value for one or more logon-related parameters, the ITS automatically sends a logon page to the Web browser. When the user has entered valid logon values, access to R/3 is granted.

- If **both** the service file for the current service **and** the global service file contain values for the logon-related parameters, but these values differ, the settings in the service file for the current service **always** override the global settings.

All logon information is stored in the ITS for the duration of a user's terminal session.

Logon Context

As described in Logon Administration [Page 7], logon information can be entered by the user, retrieved from the relevant service file, or derived from settings in the global service file. The ITS merges the logon information from all these sources and tries to establish a connection to the R/3 System. If the merged logon information is incomplete, the ITS sends a logon page and prompts the user to enter the missing information.

If a user enters at least a user name and password, this establishes a logon context comprising all the information needed to log on to an R/3 System. This context is shared among all services started from the user's workstation, so the user does not have to enter the logon information repeatedly. Instead, the ITS uses the logon information stored in the logon context, as shown in the following graphic:
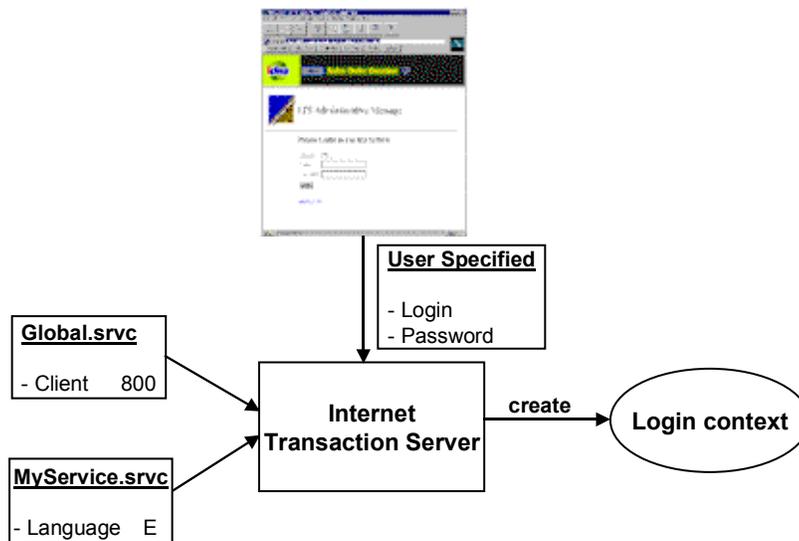

The ITS creates a logon context **only** if the user enters the user name and password. No context is created if the information is taken from service files. This is a security precaution to prevent logon information from one service file being used to start a different service, which does not make the same information available.

Logon Context Sharing

When a logon context has been successfully created, it is shared among all services started from the user's workstation.
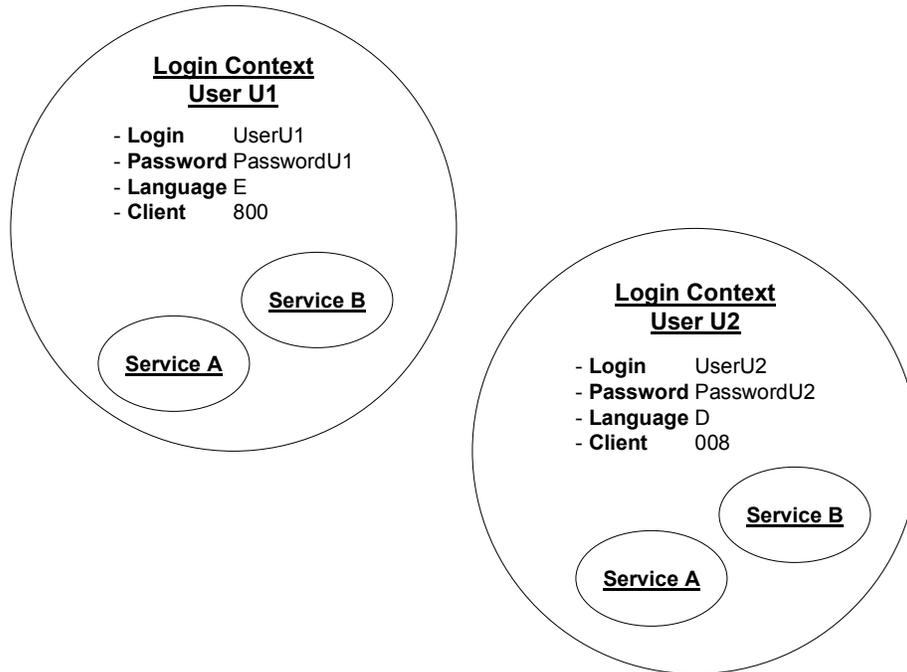
As shown in the above graphic, logon context sharing works as follows:

- If a user U_1 starts a service A for the first time, a logon context is established. If the same user then starts a service B, the ITS gets the user information from the previously created logon context to establish a connection to the R/3 System.

- If a user U_2 also starts a service A for the first time, but on a different workstation, the ITS does **not** get the user information from the logon context previously created for user U_1, because that logon context is only valid for a specific workstation.

  In this case, the ITS sends a new logon page and requests user U_2 to enter the appropriate logon information. If the information is complete and the ITS is able to establish a connection to the R/3 System, a logon context is created containing the logon information specified by user U_2. The logon context previously created by user U_1 is not affected.

Service File Conflicts

A special situation occurs when the logon information specified for a service to be started conflicts with the logon information in a logon context that has already been created.

Suppose a user U_1 logs on to a service A. In this case, the ITS creates a logon context that is shared among all services started from that user's workstation.

If user U_1 then requests a service B, but the service file for service B does not contain the logon parameters (`~login` and `~password`), the ITS uses the previously created logon context to establish a connection to the R/3 System, so the user does not have to log on again.

However, if user U_1 next requests a service C, but the service file for service C contains logon parameters for the user U_2, this constitutes a conflict with the existing logon context. In this case, the ITS sends a new logon page, which the user U_1 must complete in order to log on to R/3.

Logon Context Lifetime

To create a logon context, the following conditions must be satisfied:

- The user must enter a user name and password interactively for the first time

- The ITS must validate the information by establishing a connection to the R/3 System and successfully starting the corresponding R/3 transaction

The logon context remains active until:

- No more services are using the logon context
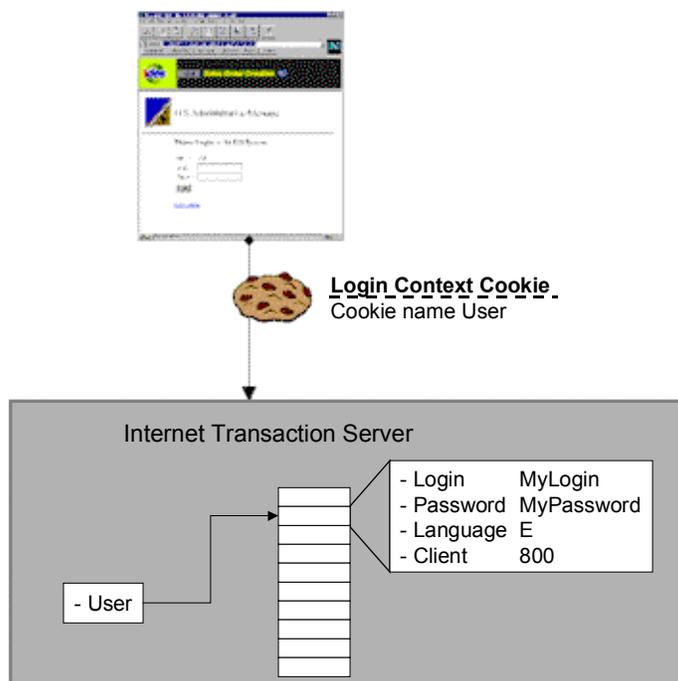
- The timeout of the logon context has expired

  You can specify the logon context timeout in the global service file by setting the value `~userTimeout` to the number of minutes you want the logon context to be kept.

When the logon context has been destroyed, the user must enter the logon information again to start a service for which there is no information stored in the service file.

The user can also log off manually by sending a command `~command=Logoff` to the ITS. For example:

`http://pal001458.pal.sap-ag.de/scripts/wgate.dll?~Command=Logoff`

When executing this command, the ITS not only destroys the user's logon context, but also disconnects all other sessions started using that logon context.

Login Context Cookie
Cookie name User

Internet Transaction Server

- Login   MyLogin
- Password MyPassword
- Language E
- Client   800

- User

Lifetime Context Cookies

When a logon context has been created, the ITS sets a value **~User** in a browser cookie. The cookie does not contain the logon information itself, but points to a data structure in the ITS.

Login Context Cookie
Cookiename User

Internet Transaction Server

- Login   MyLogin
- Password MyPassword
- Language E
- Client   800

- User