UCON RFC Basic Scenario - Guide to Setup and Operations for SAP NetWeaver 740 SP5 (and higher)

Version 3.0 | 2020 | Dr. Thomas Weiss SAP SE

THE BEST RUN SAP

Table of Contents

HOW TO USE THIS GUIDE

This section tells you which kind of information this guide offers, how to find what you want to know, and which additional information might be useful for you.

> Note:
>
> There is no need to read the whole guide. Instead, just read the sections you need, navigate to them in the way described below, and skip the rest of this document.

The best overview of the basic UCON concepts can be found in the SAP Insider article **"SAP Insider: Secure Your System Communications with Unified Connectivity"**. Go to section "UCON RFC Basic Introduction and Overview", if you want to understand what the Unified Connectivity (UCON) RFC basic scenario is good for, its basic concepts and why it is so simple. In this section you find an overview of:

- The basic tasks you need to execute in UCON setup/activation and operations,
- How the tool-supported UCON security process covers all remote-enabled Function Modules (RFMs) that are new in your system and not only the RFMs that are in the system when you run the initial UCON security classification,
- In which way UCON is suited to cope with the fact that, in general, you may want to protect PROD, but have no permission to so or do not want to execute all the UCON operations in PROD, but prefer to define in DEV which RFMs you want to expose and which to block – based on RFC logging data from PROD –, and then to transport these definitions from DEV to PROD.

Once you have an idea of how your RFC security can profit from UCON, go to section "The Different Ways to Work with the UCON RFC Basic Scenario" and make up your mind on how you want to use UCON, because there are several ways to take advantage of UCON. Next, navigate from there to the description of the respective setup that you need for your use case. In this section is also a link to a section that describes how to completely deactivate UCON and how to delete all statistical records of RFC calls persisted by UCON. After you have read how to run the setup of your use case, go to the section that describes UCON operations for the different use cases.

If you are interested in a synopsis of how to set up the different use cases including how to switch off UCON, go to section "Different Use Cases of the UCON RFC Basic Scenario in a Nutshell".

IMPORTANT UCON NOTES AND CORRECTIVE MEASURES FOR A CORRECT FUNCTIONING OF UCON

Composite SAP Note 2098702 contains the important notes for a correct functioning of UCON:

> To make sure that UCON RFC works correctly in your system have a look at the relevant notes and corrective measures in the **composite SAP Note 2098702**.

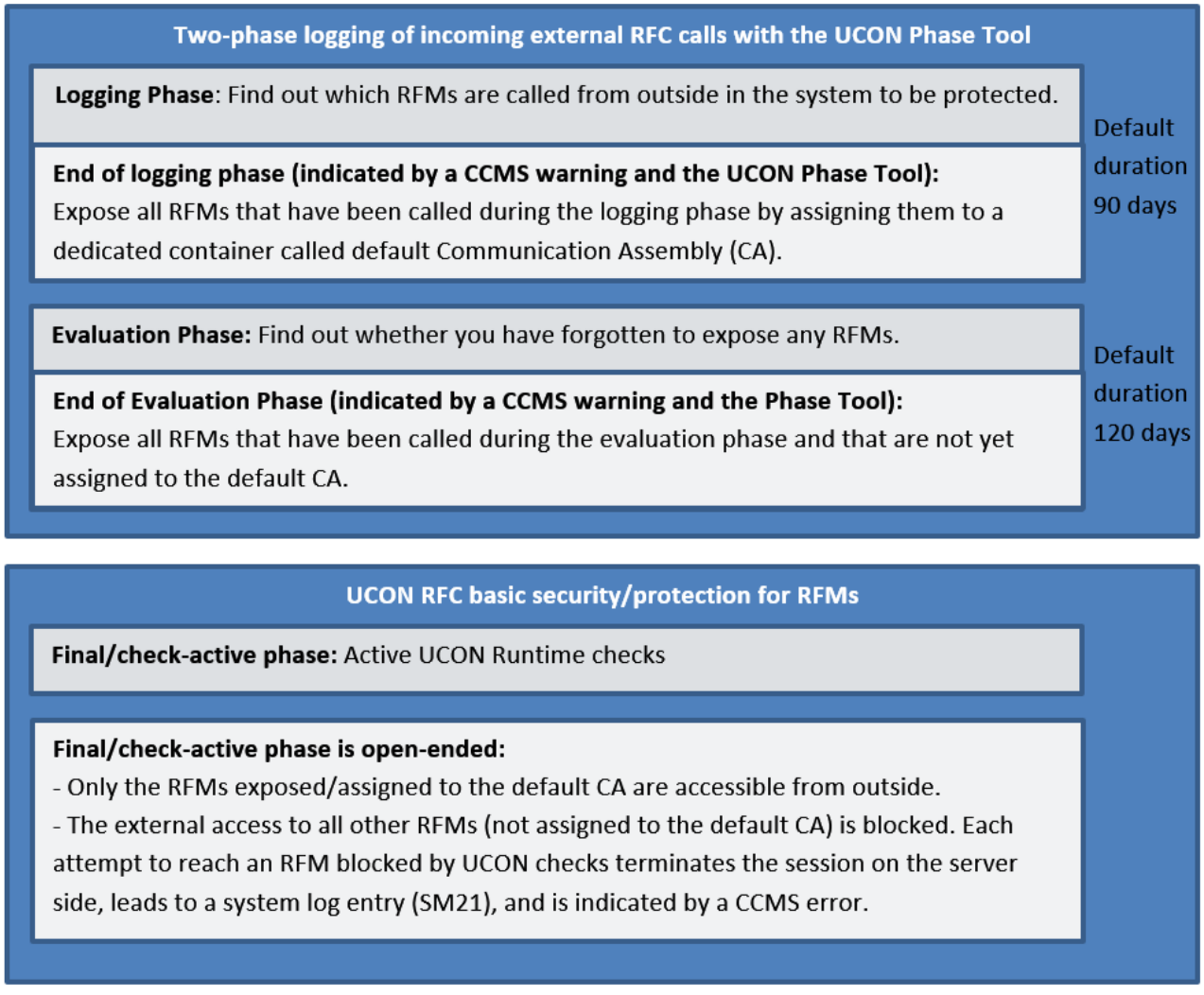
UCON RFC BASIC INTRODUCTION AND OVERVIEW

The Way UCON RFC Basic Works in a Nutshell

UCON RFC is a server-side white-list-approach for external RFC-calls that is intended to make the RFC communication more secure. The easiest way to achieve this is the UCON RFC basic scenario:

a) Find out which remote-enabled Function Modules (RFMs) need to be externally accessed from other systems or other clients in your business and technical scenarios.
b) Make the decision on which RMFs are needed for these connectivity scenarios based on a comprehensive logging of incoming external RFC calls in the UCON Phase Tool.
c) Block the external access to all other RFMs and expose only the small number of RFMs that need to be accessible from outside.

This is the way UCON RFC basic security works in a nutshell:



UCON RFC Basic Security and How to Achieve it

General Pattern of Activities Required for UCON Security (for more details go to section "How to Set up and Configure the Different UCON Scenarios")

A: **To do once**: Activate/switch on UCON RFC basic, which mainly consists of these activities:

Note: Before starting to activate/configure and run UCON, make sure that you have the authorization required to do so as described here in this guide. In particular, when running the UCON RFC Basic Scenario Landscape note that S_DEVELOP is not needed in PROD in this scenario.

1. Create the **UCON profile parameter** and set it to 1 on all relevant servers.
2. Schedule the **UCON batch job** so that all incoming RFC calls from outside are logged and persisted.
3. If your system has many servers and a high number of incoming RFC calls, chose a **shorter interval for the execution of this job** in the menu: Operations→ UCON Customizing: Reading Interval for Statistical Data.
4. Define **how long the data** of each incoming RFC call should be **stored**, which is mandatory for reasons of data privacy: Operations→ UCON Customizing: Data Privacy. After this period the respective data sets will automatically be deleted.
5. Define the **duration of logging and evaluation phase**, then run the UCON setup: Create technical entities needed for the operations of this UCON scenario and determine in which clients the UCON RFC protection should work.

Note: Choosing particular clients in the UCON setup (or in UCON setup status) only has an impact on UCON protection, not on UCON logging. Once the UCON logging is working, it logs all incoming external RFC calls – no matter in which client of the system. But as described below, it is possible to show the property "server-client" in UCON Phase Tool and to filter the list in a way that only calls are shown that arrive at particular clients.

B: **Recurrent activities**: UCON operations – general pattern:

1. Activities at the end of the logging phase:
   a. Assign all called RFMs which you want to expose to the default CA.
   b. Assign all RFMs to the evaluation phase.
2. Activities at the end of the evaluation phase:
   a. Assign all called RFMs that are not yet assigned to the default CA and that you want to expose to the default CA.
   b. Assign all RFMs to the final/check-active phase.
3. Activities during the open-ended final/check-active phase:

   Expose those RFMs blocked for external access that still have been called from outside if they are needed for your connectivity scenarios.

As you will learn in the section "UCON Protection for RFMs that are new in the System", these activities are recurrent because you should execute them:

1. Not only in the initial UCON security classification, in which you classify all RFMs that are in the system at this time,
2. But also, whenever new RFMs arrive in the system from outside by transport, installation of Support or Enhancement Packages by upgrade, or by creation within the system.

Note: UCON only controls the access to RFMs in the final phase: Only the access to an RFM that is in the final phase and that is not in the default CA is blocked by UCON.

Not passing the UCON runtime check has no effect on RFMs that are in the logging or evaluation phase. In the first two phases all RFMs are accessible. To block the access to an RFM you have assign it to the final phase without assigning it to the default CA.

Life-Cycle-Management Enablement of UCON

UCON is fully life-cycle-management enabled in two senses:

i. All RFMs that come into a system that is protected by UCON **after** the initial UCON security classification make their own way through the phases until you have classified them.
ii. UCON is suited to the restricting settings of a typical PROD system, because, in general, in a typical PROD system it will not be possible to execute standard UCON activities in the UCON Phase Tool. In particular, you cannot whitelist RFMs by assigning them to the CA, because the CA is a development object, in typical PROD-system-settings development objects cannot be changed, and nobody has sufficient authorization to change a development object there. Still, it is your PROD system that contains the most valuable data and that, therefore, needs UCON protection most.

    This is why UCON offers a scenario that enables you to relocate UCON operations to another system, normally from PROD to DEV or TEST. In order to protect your PROD system by UCON, you should collect the incoming RFC calls in PROD using the UCON logging shown in the UCON Phase Tool – an activity which does not require a developer authorization -, and copy this log to DEV or TEST. There, in DEV or PROD, you assign the relevant RFMs to the CA and the respective UCON phase, then you transport these CA- and phase-assignments of RFMs back to PROD, with the result that the RFMs in PROD will protected by the CA/whitelist that is based on the logging data of PROD. Still all relevant administrative tasks that are not allowed in a typical PROD system are executed in DEV or TEST.

UCON Protection for RFMs That Are New in the System

UCON is fully life-cycle-management-enabled in the first sense, because the three-phase process sketched above covers:

- All RFMs that are in your system when you activate UCON RFC basic.
- But also, all RFMs that later are created in or arrive in the system by transports, installation of Support or Enhancement Packages, or by upgrade.

To make the UCON security classification cover also all RFMs that are new in the system, your UCON RFC operational activities are subdivided in this way:

B1: Initial UCON RFC security classification:

After the activation of UCON, the framework assigns all RFMs in your system to the logging phase and thereby starts their way through the phases. You have to assign RFMs to the evaluation- or final/check-active phase and to the default CA (in order to expose them) **explicitly**. In general, this is not automatically done by the system (unless you select “Secure by default”, which is described in more detail in one of the notes in B2 below). At the end of the initial UCON security classification

all these RFMs have reached the final phase and are all classified as either exposed or blocked for external access. This way, only the access to RFMs in the final phase is blocked by UCON.

B2: UCON RFC security classification of RFMs that are new in the system (either created there or imported into the system): All RFMs that are new in the system are automatically assigned to the logging phase and make their own way through the phases until you have classified them based on the RFC logging data.

Note:

The **phase** is a **property of each RFM**, not a system property. In this way, new RFMs in the system can be in the logging phase, while all RFMs that are already classified can be already in the final phase.

If you need more time for the classification of a particular RFM, that is do decide as to whether to expose it or not, you can manually re-assign an RFM to the logging or evaluation phase, if it is already in the final phase, but feel unsure about this decision.

Note: Know what happens when you select **"Secure by default"** in the menu: Operations→ UCON Customizing.

This feature has the effect that all new RFMs are blocked, because they are automatically set to the final phase, but not assigned to the default CA. You should choose this feature, only if you are sure that no new RFMs needed for your RFC scenarios will arrive or be created in your system. Otherwise, if a new RFM will be an essential part of one of your RFC scenarios, this scenario will throw an UCON error, because the access to this RFM will be blocked.

Therefore, in general, selecting "Secure by default" might be risky, because it is hard to rule out the possibility that an RFM that is needed for one of your RFC scenarios arrives in your system.

B3: **Re-Assessment of RFMs blocked by UCON**, that is of RFMs which are called from outside and which are in the final/check-active phase and which do not pass the UCON runtime checks: System log entries (SM21), CCMS and UCON Phase Tool inform you about all RFMs that have been blocked by UCON so that you can assess as to whether external access to these RFMs is correctly blocked or whether you should expose or re-assign them to the logging or evaluation phase.

How UCON is Adapted to Systems in a Landscape and the Restrictions in PROD

Since the flawless working of your PROD-system(s) is crucial to your business, in general, development and many administrative activities are not allowed in PROD-systems. UCON is designed to take this basic fact about PROD-systems into account and offers you a dedicated use case to work with the UCON RFC basic scenario in your landscape:

- Protect the PROD-system based on logging data collected in PROD, but
- Make all phase- and CA-assignments of RFMs in DEV.

You can easily accomplish this with UCON:

- Copy the log of the incoming external RFC calls from PROD to DEV by exporting it to a file and importing this file into DEV.

- Transport the phase- and CA-assignments of the RFMs that you have made in DEV to PROD, using the proven ABAP transport management system.

Note: The fact that UCON is fully life-cycle-management enabled adds some flexibility, but also some complexity to the basic functioning of UCON.

Still, once you have understood the basic pattern of UCON protection (logging and blocking: In the final phase all RFMs are either blocked or exposed.), you will also easily realize the simple way RFMs make their way through the phases when there are additional process steps

- To enable the coverage of RFMs that come into the system after the initial UCON security classification,
- To suit the particular restrictions of your PROD-system.

Note: The general rule of UCON is: No Implicit Changes to the Security State of RFMs

Security is essential to your systems, and you want to stay informed about the different security features and their state in your systems. For UCON RFC basic security this means:

There are no automatic assignments of RFMs to the evaluation or final/check-active phase or to the default CA, because you should always have full control of which RFMs are protected/blocked for external access and which are exposed by UCON.

But there is a deliberate exception to this general rule, if you explicitly choose "Security by default" (SBD):

If you explicitly select SBD, all RFMs that arrive in or are created in the system after the activation of SBD are automatically assigned to the final/check-active phase, but not to the CA and are thereby blocked.

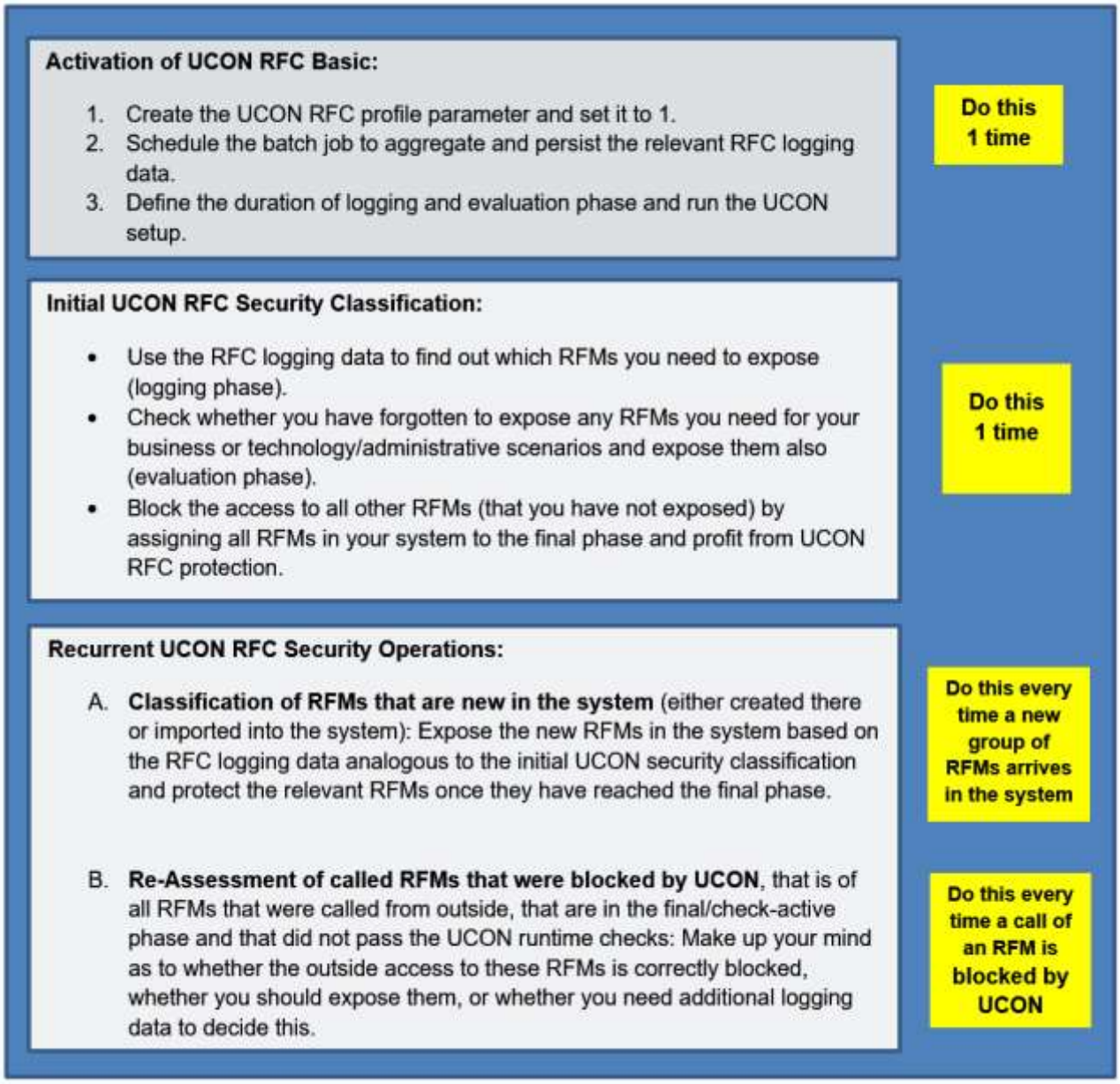
The point of SBD is to cover the following situation: You know for sure that all RFMs needed for your connectivity scenarios are exposed and all other RFMs (also the ones that arrive or are created in your system in the future) can be blocked. That means, you know that during the time SBD remains activated no RFMs arrive or are created in your system that need to be exposed.

Based on this knowledge, you can determine beforehand: All RFMS that enter the system in the next months will automatically be blocked for external access by UCON SBD.

Select this feature only, if you are sure that no new RFMs needed for your RFC scenarios arrive or are created in your system. Otherwise, if a new RFM is an essential part of one of your RFC scenarios, this scenario will throw an error, because the access to this RFM is blocked.

All in all, selecting "secure by default" might be risky, because it is hard to rule out the possibility that an RFM arrives in your system and that this RFM may be needed for one of your RFC scenarios.

UCON RFC Basic Security – Activation and Operations on One Page



Note:

There is complete UCON support and coverage, if you want to protect your PROD-system and still cannot make the required assignments there, but have to make these assignments in DEV. For this use case you must

- Activate UCON in both systems DEV and PROD and (look here for details of this process),
- Execute the relevant transport-related activities on top of the initial UCON security classification and the recurrent UCON RFC security operations: This means that you have to copy the RFC logging data from PROD to DEV and to transport the CA- and phase-assignments of RFMs from DEV to PROD (look here for details of this UCON operation process).

DIFFERENT WAYS TO WORK WITH THE UCON RFC BASIC SCENARIO

Before you customize and set up UCON you should make up your mind which way you want to use the UCON RFC basic scenario:

A. **Productive use of RFC basic scenario local**: You protect one system based on the call statistics in this system. CA- and phase-assignment of RFMs is done in this system, no transport of CA or state objects (the objects that carry the information about the phase-assignments of the RFMs) is needed. Go to detail description of the setup for this use case.

B. **Test use of RFC basic scenario local**: Same scenario as A, but only for temporary/test use. Choose this scenario if you only want to gain some practical experience with UCON for some time and want to easily deactivate it after this. As far as operations are concerned, there is no major difference between A and B. There is only a small difference in the setup between test and productive use. Go to detail description of the setup for this use case.

C. **RFC basic scenario landscape**: You want to protect only PROD, but cannot execute the required operations there. Therefore, you can collect the RFC logging data in PROD, copy them to DEV, make the CA- and phase-assignments in DEV, and then transport these assignments to PROD.
   C1. **PROD System part of RFC basic scenario landscape**: In PROD you collect the RFC logging data and it is PROD that you want to protect by UCON checks.
   C2. **DEV System part of RFC basic scenario landscape**: In DEV you make the CA- and phase-assignment of RFMs.

   As you will learn below, the setup processes in PROD and DEV are closely interconnected. Therefore, there is only one detail description for the setup in both systems DEV and PROD.

   Note: In the RFC basic landscape scenario, it is essential that all the setup-steps are executed exactly in the order described below in this guide.

D. **UCON for logging only:** You only want profit from the RFC call statistics that is provided by UCON and shown in the Phase Tool. Go to detail description of the setup of this use case.

E. **Deactivating UCON completely**: No UCON logging and no UCON runtime checks, deletion of default CA and other technical UCON entities. Go to a detail description of how to completely deactivate UCON.

AUTHORIZATIONS REQUIRED FOR UCON RFC BASIC

The authorization default values for the UCON Phase Tool, the central UCON transaction, are maintained in transaction SU24.

Note: Contrary to what is listed in transaction SU24, S_DEVELOP is **not** required in the PROD system in the UCON RFC Basic Scenario Landscape. The point of this scenario is to enable customers to use UCON with the restrictions that are typical of PROD systems. Therefore, S_DEVELOP is no need for the usage of UCON in PROD in the UCON RFC Basic Scenario Landscape. Still S_DEVELOP is **required** in

- **DEV system** in the **UCON RFC Basic Scenario Landscape** and
- **All systems** (which includes PROD systems) for the **local** UCON RFC basic scenario (As a general rule, S_DEVELOP is required in a system, where the CA is created or changed, because the CA is a development object).

As described in note 2044302, it is absolutely necessary that the job creator of the standard job SAP_UCON_MANAGEMENT has the authorization S_TOOLS_EX and the value S_TOOLS_EX_A for the authorization field AUTH. That ensures that the job creator collects the RFC server data records of **all users** using the follow-on batch job. (You should schedule this batch job for the use cases: productive and test use of RFC basic scenario local, UCON RFC basic scenario landscape, and UCON RFC for logging only.)

DATA PRIVACY PROTECTION (AS OF 7.40 SP8)

Since the UCON logging collects data about incoming RFC calls with information about the user on the client and server side, it is important that these data will be deleted after a predefined period of time for reasons of data privacy. It is mandatory to define this retention period when you set up UCON RFC basic.

Once you have defined this retention period, the UCON framework automatically deletes the relevant data records when this period has expired.

You define this period in the menu of the selection screen of the UCON Phase tool: Operations→Unified Connectivity Customizing: Data Privacy – Retention Period.

HOW TO SET UP AND CONFIGURE UCON RFC BASIC

A/B Productive and Test Use of UCON RFC Basic Scenario Local

You protect only one system based on the RFC logging data in this system. CA- and phase-assignments of RFMs are done in this system, no transport of CA or state objects needed. (Setup and configuration for productive and test use differ only in step 1.)

1. Create the UCON RFC default profile parameter *ucon/rfc/active* and set it to value 1 in transaction RZ10 for productive use (this will only become operative when the server is restarted) or in transaction RZ11 for test use of UCON.

Note:
Parameter changes via transaction RZ11 become operative at once, but get lost after a restart of the server and then overwritten by the default parameter values maintained in transaction RZ10.

Always make sure that the profile parameter "ucon/rfc/active" has the same value on each server of your system for both productive/permanent and temporary/test use of UCON.

2. Go to transaction UCONCOCKPIT (if you are on 740 SP6 or lower, transaction UCONPHTL), select "RFC Basic Scenario" under "Unified Connectivity Scenario Selection", and choose a suitable duration of the logging and evaluation phase in the menu: Operations→Unified Connectivity Customizing.

Note:

If you change the duration of the logging or evaluation phase (again) after you have run the UCON setup, this affects only RFMs that come into or are created in the system after this change, or RFMs that go into another phase (from logging to evaluation or evaluation to final) after this change.

(In any description in this guide that refers to the transaction UCONCOCKPIT it is understood that you should have selected "RFC Basic Scenario" under "Unified Connectivity Scenario Selection" in this transaction whether this is explicitly mentioned or not.)

3. In transaction UCONCOCKPIT in the "RFC Basic Scenario" navigate in the menu to: Operations→Unified Connectivity Setup:

- Choose "local Communication Assembly".
- You can protect the current client only or all clients (if desired with the exception of the customizing client 066). More specific client options can be chosen in Operations → Unified Connectivity Setup Status.
- Leave "Transport of State Objects" deselected.

Note: If all input fields in the UCON setup are greyed out, the UCON setup has already been run. In this case go to the menu: Operations →Unified Connectivity Setup Status and check if UCON is correctly configured.

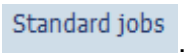
4. Maybe you want to have UCON protection only in particular clients. It is possible to activate the UCON checks in exactly those clients where you need them. In order to change the clients in which UCON is active, go to the menu: Operations →Unified Connectivity Setup Status. Under the header "Configuration of Virtual Host and Configuration per Client" you can delete and create the

configuration and the virtual host for each client: Just mark a client by selecting the respective row in the table and then choose the relevant button in the button row above the table.

Note: You can also use the UCON Setup Status window for the recreation of the default CA in case something has gone wrong with the initial creation of this entity. You get information about this failure by a message in the setup procedure, and it can also be seen by the fact that the check box with the label "default CA in all clients successfully generated" is deselected. In this case you should press the button "Generate and Save CA".

5. Schedule the UCON batch job that collects the RFC call statistics, the job "SAP_UCON_MANAGEMENT", in transaction SM36. Depending on whether the standard batch jobs of the system are already scheduled or not, there are different ways to do this:

A. The standard batch jobs are not scheduled in the system.

Execute transaction SM36 (Define Background Job), press the button 

. Further press the button 

to fill the background job name list (by default, the background job name list is empty in a new installed ABAP System), and also schedule the SAP_UCON_MANAGEMENT job, which, in turn, starts its successor jobs. The list of its successor jobs can be found in transaction SM37 (Simple Job Selection).

B. The standard batch jobs are scheduled, but the UCON standard batch job is not included in the list (probably because the batch jobs have been scheduled before).

Add the "SAP_UCON_MANAGEMENT" job to the currently existing batch jobs.

Enter the following properties for the "SAP_UCON_MANAGEMENT" job:

SAP Component = BC

Job Name = SAP_UCON_MANAGEMENT

"SAP_UCON_MANAGEMENT" starts also its successor jobs.

Since this batch job collects data about each user to whom an incoming call is assigned, the administrator who schedules this batch job needs a particular authorization (see SAP note 2044302). (Find more details on this also in section: Authorizations required for UCON RFC Basic)

The batch job log can be monitored using CCMS-monitoring (transaction RZ20).

Go to "Operations of the UCON RFC basic scenario local"

C UCON RFC Basic Scenario Landscape

You want to protect only PROD, but cannot execute the relevant UCON operations there: Therefore, you can collect the RFC logging data in PROD, copy it to DEV, make the CA- and phase-assignments in DEV, and then transport these assignments to PROD.

Note: It is necessary that you have **imported the default CA into PROD** (step 7 below) **before** you run the setup in PROD. Otherwise PROD will not work with the RFMs you expose in DEV (by assigning them to the default CA), or some other error might prevent UCON from working properly, and UCON runtime checks may interrupt productive scenarios in PROD.

In any description in this guide that refers to the transaction UCONCOCKPIT it is understood that you should have selected “RFC Basic Scenario” under “Unified Connectivity Scenario Selection” whether this is explicitly mentioned or not.

Note: Protection scope of the landscape use case:

This use case is meant to protect PROD only, because the UCON profile parameter will not be set in DEV. If you want to protect DEV also with the same CA just set the UCON profile parameter also in DEV.

Note:

Protecting PROD, DEV and/or other systems in the same landscape with the same CA only makes sense if all these different systems need to expose the same RFMs.

In general, this is not recommended because in most cases different systems do not have the same connectivity scenarios.

PROD	DEV
1. Create the UCON RFC default profile parameter *ucon/rfc/active* and set it to the value 1 in transaction RZ10. (This will only become operative when the server is restarted) **Note**: Always make sure that the profile parameter "ucon/rfc/active" has the same value on each server.	
2. Schedule the UCON batch job that collects the RFC call statistics, the job "SAP_UCON_MANAGEMENT" in transaction SM36. Depending on whether the standard batch jobs of the system are already scheduled or not, there are two ways to do this: **A. The standard batch jobs are not scheduled in the system.** Execute transaction SM36 (Define Background Job), press the button Standard jobs. Further press the button Default scheduling to fill the background job name list, (by default, the background job name list is empty in a new installed ABAP System), and also schedule the "SAP_UCON_MANAGEMENT" job and also its successor jobs. The list of its successor jobs can be found in transaction SM37 (Simple Job Selection). **B. The standard batch jobs are scheduled, but the UCON standard batch job is not included in the list (probably because the batch jobs have been scheduled before).** Add the "SAP_UCON_MANAGEMENT" job to the currently existing batch jobs.	Note: Protecting PROD, DEV and/or other systems in the same landscape with the same CA only makes sense if all these different systems need to expose the same RFMs. In general, this is not recommended because in most cases different
Enter the following properties for "SAP_UCON_MANAGEMENT" job: SAP Component = BC Job Name = SAP_UCON_MANAGEMENT "SAP_UCON_MANAGEMENT" starts also its successor jobs. Since this batch job collects data about each user to whom an incoming call is assigned, the administrator who schedules this batch job needs a particular authorization (see SAP note 2044302). The batch job log can be monitored using CCMS-monitoring (**transaction RZ20**).	Note: UCON logging starts after you have scheduled this

PROD	DEV
Note: If you change the duration of the logging or evaluation phase (again) after you have run the UCON setup this affects only RFMs that come into or are created in the system **after** this change, or RFMs that go into another phase (from logging to evaluation or evaluation to final) **after** this change.	3. Go to transaction UCONCOCKPIT (if you are on 740 SP6 or lower, transaction UCONPHTL), select “RFC Basic Scenario” under “Unified Connectivity Scenario Selection”, and choose a suitable duration of the logging and evaluation phase in the menu: Operations→Unified Connectivity Customizing. Note: 1. Add 30 days of technical buffer time (due to life-cycle-management details) to the duration you consider to be adequate. 2. The duration of the phases should be the same as in PROD.
Note: If all input fields in the UCON setup are greyed out, the UCON setup has already been run. In this case go to the menu: Operations →Unified Connectivity Setup Status and check if UCON is	4.In transaction UCONCOCKPIT (if you are on 740 SP6 or lower, transaction UCONPHTL) in the “RFC Basic Scenario” navigate in the menu to: Operations→Unified Connectivity Setup: • Choose a transportable Communication Assembly (if desired with a namespace) since you want to transport the CA to PROD. • Choose “Current Client only” under the header “Client Setup”. • Select “Transport of State Objects”. • Press the Setup button at the bottom of the window. Assign the default CA, the VHs and configurations (both are client-dependent entities), and the state objects (they carry the information about the phase-assign-ments of the RFMs) to transport requests so that you can complete the UCON setup.
	5. Release the transports with default CA, VHs and configurations, and state objects.
6. In transaction UCONCOCKPIT (if you are on 740 SP6 or lower, transaction UCONPHTL) choose a suitable duration of the logging and evaluation phase in the menu: Operations→Unified Connectivity Customizing. Note: 1. Add 30 days of technical buffer time (due to life-cycle-management details) to the duration you consider to be adequate. 2. The duration of the phases should be the same as in DEV.	Note: If you change the duration of the logging or evaluation phase (again) after you have run the UCON setup this affects only RFMs that come into or are created in the system **after** this change, or RFMs that go into another phase (from logging to evaluation or evaluation to final) **after** this change.

PROD	DEV
7. Import the transports with default CA, VHs and configurations, and state objects from DEV into PROD.	
8. Go to transaction UCONCOCKPIT (if you are on 740 SP6 or lower, transaction UCONPHTL) and select “RFC Basic Scenario” under “Unified Connectivity Scenario Selection”, navigate in the menu to: Operations→Unified Connectivity Setup, and select the same settings as in DEV: • Choose a transportable Communication Assembly and add your namespace if this is desired. (Same namespace as in DEV setup required) • You can protect the current client only or all clients (if desired with the exception of the customizing client 066). More specific client options can be chosen in Operations → Unified Connectivity Setup Status. • **At any rate make sure, that “Transport of State Objects” is de selected.** Press the *Setup* button at the bottom of the window.	Note: If all input fields in the UCON setup are greyed out, the UCON setup has already been run. In this case go to the menu: Operations →Unified Connectivity Setup Status and check if UCON is correctly configured. Note: Selecting “Transport of State Objects” would lead to an error message: It would trigger a transport request dialogue window, but due to normal PROD-settings, you would just get this error message, because of missing authorizations and because dev objects are not changeable there. Since the very purpose of the landscape scenario is to enable UCON despite of normal PROD settings, avoid this by always deselecting “Transport of State Objects”.
9. Maybe you want the UCON checks only in particular clients. It is possible to activate the UCON checks in exactly the clients you need them. If you want to change the clients in which UCON is active, go to the menu: Operations →Unified Connectivity Setup Status. Under the header “Configuration of Virtual Host and Configuration per Client” you can delete and create the configuration and the virtual host for each client: Just mark a client by selecting the respective row in the table and then choose the relevant button in button row above the table.	

Go to “UCON RFC basic scenario landscape -- Operations”

D UCON RFC for Logging Only

You only want to profit from the RFC call statistics that is shown in the UCON Phase Tool, but are not interested in UCON protection.

Note: In any description in this guide that refers to the transaction UCONCOCKPIT it is understood that you should have selected “RFC Basic Scenario” under “Unified Connectivity Scenario Selection” in this transaction whether this is explicitly mentioned or not.

1. Go to transaction UCONCOCKPIT (if you are on 740 SP6 or lower, transaction UCONPHTL) and select “RFC Basic Scenario” under “Unified Connectivity Scenario Selection” and navigate in the menu to: Operations→Unified Connectivity Setup:

- Choose a local Communication Assembly.
- Select “Current client only” under the header “Client Setup”.
- Leave “Transport of State Objects” deselected.

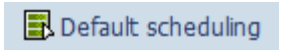
Note: If all input fields in the UCON setup are greyed out, the UCON setup has already been run. In this case go to the menu: Operations →Unified Connectivity Setup Status and check if UCON is correctly configured.

2. If there was an error message in the setup, go to the menu: Operations →Unified Connectivity Setup Status and recreate the default CA. This error can also be seen by the fact that in the Unified Connectivity Setup Status window the check box with the label “default CA in all clients successfully generated” is deselected. In this case you should press the button “Generate and Save CA”.

3. Schedule the UCON batch job that collects the RFC call statistics, the job “SAP_UCON_MANAGEMENT” in transaction SM36. Depending on whether the standard batch jobs of the system are already scheduled or not there are two ways to do this:

A. The standard batch jobs are not scheduled in the system.

Execute transaction SM36 (Define Background Job), press the button 

. Further press the button 

to fill the background job name list (by default, the background job name list is empty in a new installed ABAP System) and also schedule the “SAP_UCON_MANAGEMENT” job and also its successor jobs. The list of its successor jobs can be found in transaction SM37 (Simple Job Selection).

B. The standard batch jobs are scheduled, but the UCON standard batch job is not included in the list (probably because the batch jobs have been scheduled before).

Add the “SAP_UCON_MANAGEMENT” job to the currently existing batch jobs.

Enter the following properties for the “SAP_UCON_MANAGEMENT” job:

SAP Component = BC

Job Name = SAP_UCON_MANAGEMENT

“SAP_UCON_MANAGEMENT” starts also its successor jobs.

Since this batch job collects data about each user to whom an incoming call is assigned, the administrator who schedules this batch job needs a particular authorization (see SAP note 2044302).

The batch job log can be monitored using CCMS-monitoring (transaction RZ20).

Go to “Operations of UCON Logging”.

E Completely Deactivating UCON RFC Basic

No UCON logging and no UCON runtime checks, no default CA or any other UCON-related entities.

1. Set the UCON RFC default profile parameter *ucon/rfc/active* to 0 in transaction RZ11 and also in transaction RZ10 if you want to deactivate the UCON checks immediately. If you have used UCON only for testing and therefore have only set the temporary profile parameter, only use transaction RZ11.

Note: Always make sure that the profile parameter “ucon/rfc/active” has the same value on each server.

2. To delete the UCON entities such as default CA, VH and all the state objects of the RFMs go to transaction UCONCOCKPIT (if you are on 740 SP6 or lower, transaction UCONPHTL) and choose in the menu: Operations→ UCON Reset. In a subsequent window you may choose to also delete all the RFC logging data collected and persisted by UCON.

F The Different Use Cases of the UCON RFC Basic Scenario in a Nutshell

Use Case	Scope of Use Case	Value of UCON Profile Parameter (UCON/RFC/ACTIVE)	UCON Runtime Checks	Configure Default CA, Def. Host and Def. Conf. in at Least One Client	Schedule UCON Batch Job	Logging of External RFC Calls
A. Productive use of RFC basic scenario local	Runtime checks, logging of RFC calls, and phase- and CA-assignment in one system for **permanent use**	1 (default parameter in RZ10 recommended, system restart required)	Yes	Yes	Yes	Yes
B. Test use of RFC basic scenario local	Runtime checks, logging of RFC calls, and phase- and CA-assignment in one system **for temporary use**: You can switch off UCON without server-restart	1 (temporary parameter in RZ11 recommended, no system restart required)	Yes	Yes	Yes	Yes
C1. PROD System part of RFC basic scenario landscape	Runtime checks, logging of RFC calls, **no** phase- and CA-assignment in PROD (Note: Setup processes in DEV and PROD are closely interconnected in this scenario)	1 (default parameter in RZ10 recommended, system restart required)	Yes	Yes	Yes	Yes
C2 DEV System part of RFC basic scenario landscape:	**No** runtime checks and **no** logging of RFC calls, **but** phase- and CA-assignment in DEV (Note: Setup processes in DEV and Prod are closely interconnected in this scenario)	0 (default parameter in RZ10 recommended, system restart required)	No	Yes	No	No
D Logging only	**No** runtime checks, logging of RFC calls, **no** phase- and CA-assignments (Two different ways to configure and set up this use case)	0 (default parameter in RZ10 recommended, system restart required)	No	Yes	Yes	Yes
UCON RFC completely switched off	No UCON entities at all, no runtime checks	0 (default parameter in RZ10 recommended, system restart required)	No	No	No	No

OPERATIONS OF UCON RFC BASIC

A/B Productive and Test Use of UCON RFC Basic Scenario Local

These are the operations you should perform in order to make your RFC connectivity more secure with the UCON RFC basic scenario, if you log the RFC calls and make the CA- and phase-assignments of RFMs in one system so that you can protect this system.

1. **Initial UCON security classification of RFMs** based on UCON logging data (these process steps are performed once per system until all RFMs that are in your system at a given time are either classified as exposed or blocked by UCON):
   - After the UCON setup, the RFMs in the system are automatically assigned to the logging phase.
   - At the end of the logging phase, you should perform some actions. (In transaction RZ20 under SAP UCON Monitor Templates you find the work list for the UCON Phase Tool.)

Note: If you do not use transaction CCMS, UCON still informs you about the expiration of logging and evaluation phase: Just select “Display RFMs with Status ‘expired’ only” in the Phase Tool and you see the RFMs with an expired logging or evaluation phase below.

Activities at the end of the logging phase:

- If a group of RFMs has reached the end of the logging phase, you get a warning in the relevant node in transaction RZ20.
- By double-clicking this node, you reach a list in the UCON Phase Tool that shows all RFMs with an expired logging phase.
- Navigate to the Phase Tool selection screen (if you are on 740 SP6 or lower, open the selection screen of the phase tool (transaction UCONPHTL) in a new session), select “Called Function Modules without CA assignment” and restrict the selection to those RFMs with an expired logging phase.
- Next you have two options:
  - If you have the time and knowledge to analyze the called RFMs, press the button “More/less displayed fields” (or SHIFT + F7) and drill into more details of the RFMs that have been called. Based on this information, mark only the RFC calls that you consider to be legitimate.
  - If you lack time or the knowledge needed for an analysis of these RFC calls, mark all entries in the list of called RFMs without CA-assignment.
- Assign all marked RFMs to the default CA.
- Navigate back to the selection screen and select “Function Modules in logging phase”. (The property “Display RFMs with status ‘expired’ only” should still be selected.)
- Assign **all** RFMs from the logging to the evaluation phase (not only those that have been called).

Activities at the end of the evaluation phase:

- If a group of RFMs has reached the end of the evaluation phase, you get a warning in the relevant node in the CCMS.
- The activities required at the end of the evaluation phase are analogous to those at the end of the logging phase: Again you navigate from the CCMS to the list in the UCON Phase Tool, mark the called RFMs at the end of the evaluation phase, assign them

(with or without analysis) to the default CA, and assign **all** RFMs with an expired evaluation phase (those that have been called **and** those that have not been called) to the final phase.

2. **Control of RFC calls that are rejected,** because they do not pass the UCON runtime checks. (These process steps need to be executed every time the relevant node in the SAP UCON Monitor Templates shows that an RFC call has been blocked by UCON.)
   - Again, go to transaction RZ20, and under SAP UCON Monitor Templates you find the work list for the UCON Phase Tool.

   Note: If you do not use the CCMS, UCON still informs you about rejected calls: Under the header "Function modules in final phase" the "called Function modules without CA assignments" are the RFC calls rejected by UCON.

   - If there are any RFC calls that were rejected because of the UCON runtime checks, the relevant node in the SAP Unified Connectivity Monitor Templates shows an error.
   - By double-clicking the relevant node, you get to the UCON Phase Tool. (You can also detect these rejected RFC calls by choosing the respective selection on the Phase Tool selection screen.)
   - If any of these rejected RFC calls should not be blocked by UCON, mark the relevant RFMs and assign them to the default CA or (if you are not sure about this) re-assign the relevant RFMs to the logging or evaluation phase.
3. **Ongoing classification of RFMs that are new in the system (**no matter if they arrive there by transports, SP- or EhP-Installation or if they are newly developed in the system): They are automatically assigned to the logging phase. (The following process steps need to be performed every time RFMs are new in the system.)

   The relevant activities in transaction RZ20 (if you do not use the CCMS just look in the Phase Tool to get informed about the expiration of logging and evaluation phase as described above) and in the UCON Phase Tool are by and large the same as described above in the initial UCON security classification of RFMs based on UCON logging data. But some minor short cuts are possible in the process of classifying new RFMs: If the list in the UCON Phase Tool shows only a small number of RFMs at the end of the logging or evaluation phase, you may save time by manually selecting and marking the RFMs you want to assign to the default CA without going back to the selection screen of the UCON Phase Tool.

   You may also simplify the process by making the necessary assignments in the UCON Phase Tool for different groups of RFMs (with different expiration dates for each group) together. But, of course, the simplest way to achieve UCON protection for each RFM or group of RFMs is to make the necessary assignments in the UCON Phase Tool as soon as the relevant phase for this RFM or group of RFMs is expired.

C UCON RFC Basic Scenario Landscape

These are the operations you should perform in order to make your RFC connectivity more secure with the UCON RFC basic scenario, if you want to protect only PROD, but cannot execute the relevant UCON operations there: So you can collect the RFC logging data in PROD, copy it to DEV, make the CA- and phase-assignments in DEV, and then transport them to PROD.

Note: The UCON data shown in transaction RZ20 under SAP UCON Monitor Templates are always based on the local data of the respective system, while the UCON Phase Tool (transaction UCONCOCKPIT for releases >= 740 SP7 and transaction UCONPHTL for releases < 740 SP7) can show the RFC logging data from the local or from other systems depending on your choice.

- Since you are interested in the end of the logging or evaluation phase in PROD, always use the CCMS in PROD to find out whether the respective phase is expired for a group of RFMs in PROD.
- If you do not use CCMS, UCON still informs you about the expiration of logging and evaluation phase: Just select "Display RFMs with Status 'expired' only" in the Phase Tool and you see if there are RFMs with an expired logging or evaluation phase below in this tool.

1. **Initial security classification of RFMs based on UCON RFC logging data** (these steps are performed once until all RFMs in the system at this time are classified as exposed or blocked):

PROD	DEV
After the UCON setup, the RFMs in a system are automatically assigned to the logging phase. **Activities at the end of the logging phase:** The relevant screen of transaction RZ20 informs about the phase expiration and shows the number of RFMs for which the logging phase is expired. You find this in the "Work list for UCON Phase Tool" in transaction RZ20 under "SAP UCON Monitor Templates": When a group of RFMs has reached the end of the logging phase you get a warning. Start transaction UCONCOCKPIT (if you are on 740 SP6 or lower, transaction UCONPHTL) and choose in the menu: Operations → Statistical Records → Export Statistics Records to save the RFC logging data to a file.	
	Import the RFC logging data in transaction UCONCOCKPIT (or transaction UCONPHTL for releases lower than 740 SP7) and choose in the menu: Operations → Statistical Records → Import Statistics Records.

	In the UCON Phase Tool (transaction UCONCOCKPIT or transaction UCONPHTL for releases lower than 740 SP7) under the header “Use Statistics from System” choose the SID of your PROD-system. This way the Phase Tool will show a selection from the RFC logging data of PROD.
	Select “Display RFMs with status ‘expired’ only” (to show only RFMs with an expired logging phase) and below “Function Modules in logging phase” choose “called Function Modules without CA assignment” and press the EXECUTE button.
	Next you have two options: • If you have the time and knowledge to analyze the called RFMs, press the button “More/less displayed fields” (or Shift + F7) and drill into the details of the RFMs that have been called. Based on this information, mark only the RFC calls that you consider to be legitimate. • If you lack the time or the knowledge needed for an analysis of these RFC calls, mark all entries in the list that shows the called RFMs without CA-assignments.
	Assign all selected RFMs to the default CA and choose a transport request for the CA before saving your changes.
	Navigate back to the selection screen and select “Function Modules in logging phase”. (The property “Display RFMs with status ‘expired’ only” should still be selected.)
	Assign all RFMs to the evaluation phase and choose a transport request for the state objects before saving your changes (state objects contain the information about the phase-assignment of the RFMs).
Note: It is important that you assign **all** RFMs with an expired phase to the next phase, not only the RFMs that have been called. When to assign an RFM from the logging phase to the next phase depends only on the expiration date of the logging phase. It is completely independent of whether an RFM has been called or not.	
In DEV, release the transport with the relevant state objects and the transport with the default CA and import them into the PROD-system.	
After the import of the default CA and the RFC state objects into PROD, the relevant RFMs in PROD (as in DEV) are in the evaluation phase, and a subset of them is assigned to the default CA.	

Note: Transporting the default CA and the state objects of all RFMs from DEV to PROD in due time makes sure that CA- and phase-assignments of RFMs are in sync between DEV and PROD.

PROD	DEV
Activities at the end of the evaluation phase: The relevant screen of transaction RZ20 informs about the phase expiration and shows the number of RFMs for which the evaluation phase is expired. You find this in the "Work list for UCON Phase Tool" in transaction RZ20 under "SAP UCON Monitor Templates". When a group of RFMs has reached the end of the evaluation phase you get a warning. Start transaction UCONCOCKPIT (if you are on 740 SP6 or lower, transaction UCONPHTL) and choose in the menu: Operations → Statistical Records → Export Statistics Records to save the RFC logging data to a file.	
	In transaction UCONCOCKPIT (if you are on 740 SP6 or lower, transaction UCONPHTL) import the data by choosing in the menu: Operations → Statistical Records → Import Statistics Records.

PROD	DEV
	Under the header “Use Statistics from System” choose the SID of your PROD-system. This way the Phase Tool will show a selection from the RFC logging data from PROD.
	Select “Display RFMs with status ‘expired’ only” (to show only RFMs with an expired evaluation phase) and below “Function Modules in evaluation phase” choose “called Function Modules without CA assignment” and press the EXECUTE button.
	Next you have two options: • If you have the time and knowledge to analyze the called RFMs, press the button “More/less displayed fields” (or Shift + F7) and drill into the details of the RFMs that have been called. Based on this information, mark only the RFC calls that you consider to be legitimate. • If you lack the time or the knowledge needed for an analysis of these calls, mark all entries in the list that shows the called RFMs without CA-assignments.
	Assign all marked RFMs to the default CA.
	Navigate back to the selection screen and select “Function Modules in evaluation phase”. (The property “Display RFMs with status ‘expired’ only” should still be selected.)
	Assign **all** RFMs to the final phase and choose a transport request for them.
Note: It is important that you assign **all** RFMs with an expired phase to the next phase, not only the RFMs that have been called. When to assign an RFM from the evaluation phase to the final phase depends only on the expiration date of the evaluation phase. It is completely independent of whether an RFM has been called or not.	
Release the transport with the relevant state objects and the transport with the default CA and import them into PROD.	
After the import of the default CA and the RFC state objects into PROD the relevant RFMs in PROD (as in DEV) are in the final phase and a subset of them is assigned to the default CA.	
Note: Transporting the default CA and the state objects of all RFMs to PROD in due time makes sure that CA- and phase-assignments of RFMs are always in sync between DEV and PROD.	

2. **Control of RFC calls that are rejected because they do not pass the UCON runtime checks** (These process steps need to be executed every time the relevant node in the SAP

UCON Monitor Templates in PROD shows an error, that is every time when an RFC call has been blocked by UCON.)

- Again, in PROD, go to transaction RZ20, and under SAP UCON Monitor Templates you find the “work list for the UCON Phase Tool”.

Note: If you do **not** use CCMS, still, System Log (SM21) and UCON Phase Tool inform you about rejected calls: Under the header “Function modules in final phase” the “called Function modules without CA assignments” are the RFC calls rejected by UCON.

- If there are any rejected RFC calls that did not pass the UCON runtime checks because the called RFM is in the final phase, but not in the default CA, the relevant node in the SAP Unified Connectivity Monitor Templates shows an error.
- If all or some of these RFMs that have been blocked by UCON should be accessible for external calls, you have two options to achieve this:
    - If only one or a small number of RFMs is affected, you can go directly to the UCON Phase Tool in DEV, select and mark the relevant RFMs, assign them to the default CA and transport the default CA to PROD.
    - The way to handle a large number of RFMs is to copy the RFC call statistics from PROD to DEV (in the same way as described above under 1), to select the called RFMs without CA-assignment in the final phase, to assign them to the default CA, and then to transport the default CA from DEV to PROD.

If you are unsure as to whether to expose or block a rejected RFM, you can re-assign it to the logging or evaluation phase in DEV and transport the state objects to PROD. This way you can re-evaluate this RFM.

3. Ongoing classification of RFMs that are new in the system (no matter if they arrive there by transports, SP- or EhP-Installation, or if they are newly developed): The framework automatically assigns them to the logging phase. (These process steps need to be executed every time new RFMs arrive or are created in your UCON-protected system)

   The activities in transaction RZ20 and in the UCON Phase Tool are by and large the same as described above under 1 in the initial security classification of RFMs based on the UCON RFC logging data. There are only some minor short cuts that may help to make the process simpler.

   Again, it is always the CCMS in PROD where you should check whether the logging or evaluation phase is expired for a number of RFMs.

   Note:
   If you do not use CCMS, UCON still informs you about the expiration of logging and evaluation phase: Just select “Display RFMs with Status ‘expired’ only” in the Phase Tool and you see if there are RFMs with an expired logging or evaluation phase below in this tool.

   If the list of RFMs with an expired phase is short, you may save time by making the necessary assignments in the Phase Tool in DEV without copying the RFC call statistics from PROD to DEV. That is, you assign the subset of RFMs that have been called with or without further analysis to the default CA, you assign all RFMs with an expired logging or evaluation phase to the next phase, and then you transport the default CA plus the state objects from DEV to PROD.

If the list of RFMs with an expired phase is longer, you should copy the RFC call statistics from PROD to DEV and make the assignments there in the way described above.

In any case, you should transport the CA and the relevant state objects from DEV to PROD after you have made the relevant assignments.

Note:
When you assign RFMs from the evaluation to the final phase, always make sure that you first make the assignments to the default CA before you assign the RFMs to the final phase.

You may also simplify the process by making the necessary assignments in the UCON Phase Tool for different groups of RFMs (with different expiration dates for each group) together. But, of course, the simplest way to UCON protection for each RFM or group of RFMs is to make the necessary assignments in the UCON Phase Tool immediately as soon as the relevant phase for this RFM or group of RFMs is expired.

D UCON RFC for Logging Only

If you just want to profit from the perspicuous UCON logging without UCON runtime checks (and without the phase- and CA-assignments needed to make UCON protection work properly), go to transaction UCONCOCKPIT (if you are on 740 SP6 or lower, transaction UCONPHTL), select “RFC Basic Scenario” under “Unified Connectivity Scenario Selection”, and choose the selection that fits your needs. Since you do not have a Communication Assembly nor assign any RFMs to phases you can ignore all predefined selections that refer to these entities.

On the subsequent screen you see a list of called RFMs with some relevant attributes. By pressing the respective button, you can also see more attributes for called RFMs.

FAQ

1. What about New Scenarios, Which Might Need Access to RFMs that Are Already Blocked by UCON?

As already told, UCON protection automatically covers RFMs that are new in the system: They are automatically assigned to the logging phase. But what about the situation when your company wants to use a scenario

- That has so far not been implemented in the relevant system and
- That might need external access to RFMs which are already in the system and which have been blocked by UCON because they are not needed by the scenarios run so far in the relevant system.

As a matter of fact, you need to find out if any -- and if so which -- RFMs need to be accessed by a new scenario before you run this scenario in your PROD-system. Therefore, you should evaluate the new scenario with all the connectivity it needs in a test system:

- Implement the complete new scenario in a test system in your landscape (with all connections to other systems that are needed for the scenario. Ideally, the test system and the other systems needed for the new scenario are in an isolated sub-network or in a sub-network that is as isolated as possible. This isolation ideally should prevent incoming RFC calls that do not belong to the new scenario you want to run in the test system).
- Make sure that this test system uses the same default CA as the relevant system protected by UCON, which means that you have the same RFMs exposed and the same RFMs protected in the test system as in this system. (Set up UCON RFC basic in the test system and transport the default CA from the relevant system that is protected by UCON to this test system. You can transport the default CA as described above in the UCON setup of the UCON RFC Basic Scenario Landscape. Just note that the transport may have another source and target system than in the description.)
- Run the new business scenario in your test system over such a period of time that all sub-scenarios you need for your business have run a least once.
- Look in the UCON Phase Tool or the CCMS in your test system to find out which RFMs have been accessed from outside, but have been blocked/rejected by UCON.
- Allow the access to these RFMs in the relevant system that is protected by UCON. You do this by re-assigning these RFMs to the logging phase. Make sure that the duration of the logging and evaluation phase in your PROD-system is long enough and check whether these RFMS are called during this scenario.
- After these relevant RFMs have been called during the logging or evaluation phase, assign them to the default CA and the subsequent phases as described above under UCON RFC Basic Scenario Landscape or UCON RFC Basic Scenario Local depending on the way the relevant system is protected by UCON.

2. Does Setting the UCON Profile Parameter and Configuring UCON Already Enhance the RFC Security of Your System, or Are There More Activities Needed to Achieve This?

Setting the UCON profile parameter plus running the UCON setup switches the UCON machinery on, but, at first, does not enhance the security of the respective system: Activation and setup of UCON means that now UCON collects and persists the RFC call statistics. Based on these data you can decide whether to expose or block a particular RFM.

Still, switching on UCON does not block anything on its own. Since you will only enhance the RFC security of your system if the access to a number of RFMs is blocked, you need more than just setting the UCON profile parameter and running the UCON setup.

Why is this so? No RFM in the logging or evaluation phase is blocked. It is only in the final phase that the UCON runtime checks control the access to some RFMs: In the final phase only the RFMs in the default CA (the UCON white list) are externally accessible, and the access to all other RFMs in the system is blocked. In the logging and evaluation phase the UCON runtime checks are only simulated. This means: Access to RFMs that do not pass the UCON runtime checks is not blocked if these RFMs are in the logging or evaluation phase.

UCON RFC is deliberately designed this way: Though you need no particular semantic knowledge about the RFMs in your system to profit from UCON RFC security, you still have to make up your mind on which RFMs you need to expose. So, where to get the knowledge from, the knowledge that you need to justify this decision: It is the UCON log in the Phase Tool that gives you the information you need to find out which RFMs you need to expose, before you block the access to all the other RFMs. Just use the first and second phase (in which the runtime checks are only simulated so that no RFMs are blocked) to find out which RFMs are called from outside by looking at the UCON RFC log in the UCON Phase Tool. Assuming that

- You have chosen a suitable duration of the logging and evaluation phase and
- The RFMs called in these two phases will also be called from outside in the future

you should assign these called RFMs to the default CA: At the end of the evaluation phase you should be sure that you have assigned all the RFMs that are needed for your connectivity scenarios to the default CA. Then you assign all RFMs to the final phase, and it is only then that the access to a lot of RFMs (all that are not in the default CA) is blocked.

Note:
Logging and evaluation phase should cover a period of time in which all regular and legitimate business and technical/administrative scenarios in your company have run at least once, ideally plus some time reserve. You extrapolate the RFC call statistics of these two phases into the future: Unless new scenarios are implemented in your system, you should be sure that this approach finds all RFMs you need to expose. (If you implement a new scenario in a system already protected by UCON you should keep in mind the answer to question 1 above and act accordingly.)

In general, end of the year should also be covered by logging or evaluation phase, because certain scenarios may only run at this time of the year.

Note:

If you have doubts as to whether the external call of an RFM during the logging or evaluation phase was legitimate or not, and/or if you have the intention, time, and knowledge to analyze a particular call of an RFM, go to the result screen in the UCON Phase Tool that shows the relevant RFM, press the button “More/Less Displayed Fields”, and analyze this call based on properties like calling system, caller user etc.

So, once you are sure about which RFMs to expose, you assign them to the default CA, and then assign all RFMs from the evaluation to the final phase. This allows external access to only the RFMs in the default CA and blocks access to all other RFMs.

In general, there is no automatic assignment of RFMs to the evaluation or final phase. It is up to you to make the relevant assignments (except for the “secure by default” mode of UCON). This is why there is no automatic blocking of RFMs by UCON and why merely switching on UCON has no impact on the security of your connectivity scenarios. Normally, before the access to any RFM is blocked you have to manually assign this RFM to the final phase.

You need not be afraid that just activating UCON by setting the relevant profile parameter and running the UCON setup will inadvertently block any RFMs. It is you who decides about when to assign an RFM to the evaluation or final phase. And it is only after assigning RFMs to the final phase that the access to an RFM will be blocked by UCON if this RFM is not assigned to the default CA.

3. “I have scheduled the UCON RFC batch job, but still no RFC call statistics is collected.”

The UCON batch jobs only collects data

- If the UCON RFC batch job is scheduled and
- If the UCON setup has run in at least one client and/or in transaction RZ10.

(for all details cf. this section).

4. “How Do I find a suitable length for the logging and evaluation phase?”

The logging or first phase should cover a period such that all your technical and business RFC scenarios and their relevant sub-scenarios have at least once run once within the logging phase. In general, this means that the end of year should also be part of the logging phase. Since the scheduling of these scenarios depends on the concrete customer, there can be no general rule for the length of the first phase.

The aim of the second or evaluation phase is to have a period in which you can try out whether you have assigned all the relevant remote enabled function modules (RFMs) to the default CA, and its duration should be long enough to check whether you have forgotten to expose an RFM that is needed for a scenario. Again, SAP can give no recommendations for the length of this phase, but the duration depends upon you, the scenarios in your system and how cautious you are.

There is a general trade-off between improving your RFC security by means of UCON RFC soon and avoiding to stop a business process unintentionally by blocking the access to a relevant RFM that is needed for the respective process: The shorter the duration of the logging and evaluation phase is, the earlier you can have your RFMs protected by UCON, but the larger is the risk that you might have overlooked an RFM that you need to expose. The longer the duration of these phase is, the lower is the risk to overlook an RFM that needs to be called from outside, the later

you get the UCON protection of the RFMs. In general, it is up to you and your experts to find the right balance between these conflicting objectives, when using UCON RFC.

It makes the process easy to manage, if you assign all RFMs to the 2nd phase, when their first phase is expired, and the same is true in an analogous way for the assignment the 3rd phase. You can call this the UCON-driven assignment of RFMs to phases, because the time for the assignment to the next phase is calculated by UCON based on the respective phase duration that you have defined and the time an RFM entered the respective phase. The UCON phase tool shows you when the logging- or evaluation phase is expired for one or many RFMs, and at that time you should assign them to the next phase. (Again, remember that the phase is a property of each RFM, not of the system.)

You define the duration of the first and the second phase for all RFMs in the system, but for each RFM such a phase starts at the point in time when it is assigned to this phase. Still, you can have a shorter or longer duration of a phase for some RFMs by manually assigning these RFMs to another phase or re-assigning them to same phase at any time you want (when re-assigning an RFM to the same phase, the phase starts a new.) With these manual assignments you can also skip a phase for some RFMs and assign them from the 1st to the 3rd phase or re-assign RFMs from the 3rd phase back to the 2nd phase. In contrast to the UCON-driven automatic assignment, you can call this the free or manual assignment of RFMs, because it is up to you to which phase you assign an RFM and when you do this.

What is the point of these free assignments of RFMs to a UCON phase?

i. If you are sure that you want to block some RFMs with UCON (maybe because they are very critical and, therefore, should never be called from outside) no matter whether they are called or not from outside during the duration of the logging and evaluation phase, assign them from the 1st to the 3rd phase, without assigning them to the default CA.

ii. An RFM in the 3rd phase that is blocked (not assigned to the CA), is still called from outside. If you want to find out whether this RFM is called on a regular base and legitimately or whether the respective RFM has just been called one time in an unauthorized way or by accident, re-assign it to the 1st phase, and again you have the whole 1st and 2nd phase to watch how often the relevant RFM is called, before you decide to whitelist it or not to do so.

iii. For some reason you suspect that an RFM which is in the CA and in the 2nd (evaluation) phase should still be blocked. A good way to find out whether the relevant RFM needs to be called from outside on a regular base is to remove this RFM from the CA and re-assign to the first (logging) phase. Then the logging phase starts anew, and you can look if the relevant RFM is called from outside during the whole logging phase. At the end of the logging phase of this RFM, you assign it to the evaluation phase, and if it is still has not called from outside until the end of the evaluation phase, you assign it to the final phase. Then the relevant RFM is blocked, because all RFMs that are in the final phase and that are not part of the CA are not accessible from outside.

It is good practice for customers to take sufficient time to think about and discuss the suitable length of these phases for a landscape or a larger unit, then to decide, implement the decision, and to maintain this decision. In general, exceptions to the normal phase process such as the cases described above under i to iii should be implemented by free assignments of the respective RFMs to another phase, not by repeated changes of the phase duration.

As a general rule, it is advised to avoid repeated changes of the duration of the UCON phases, because you might easily lose control of which group of RFMs has which phase duration and thereby in the end not even know how long a particular RFM was in which phase. This problem of losing oversight by changing the phase duration is aggravated by the fact that simply changing the general duration of a phase in the UCON phase tool does not have an effect on all RFMs, but only on the RFMs that get assigned to the relevant phase after this change. For example, changing the duration of the logging phase again some weeks after having configured UCON would have no effect at all on each RFM that is already in the logging phase, but only on the RFMs that get newly

assigned to the logging phase after this change. Accordingly, it would be difficult to know how long a particular RFM has been in the logging phase at the point in time when this phase is expired for this RFM – most probably you will not know which phase duration was selected at the time when the respective RFM entered the logging phase.

Though you should not plan a process that envisages repeated changes of the duration of the UCON phases, there is one reason why you still should change phase duration: For some reason or other you might have miscalculated the period of time you need for the logging phase. For example, you might have selected 180 days as the duration of the logging phase, and later you get to know that there are scenarios in your system that run only once a year. In this case, the best solution is to change the general duration of the logging phase. But in these cases you must also make sure that this change also has an effect on the RFMs that are already in this phase: In order to achieve this, in the selection screen of the UCON phase tool select all RFMs that are in the logging phase, mark them all on the result screen, and reassign them all to the logging phase.

How can you monitor more properties of incoming RFC calls in UCON Phase Tool?

In the standard view of the result screen in the UCON Phase Tool you can select these columns in the user interface that shows the logged RFC calls:

Function module name, *phase*, *Communication Assembly*, *phase expiration date* (When is the respective phase of the RFM expired?), *counter* (How many times has the RFM been called?), *counter other system* (How many times has the RFM been called from other systems?), *counter same system* (How many times has the RFM been called from other clients of the same system?), SBD (Secure by default: Is the respective RFC blocked by UCON, because it arrived in the system or was developed there at a time, when SBD was selected for the system) *date of first call*, date of last *call*.

You can toggle between this standard view and a view with more detail information by selecting the button “Fields” on the right above the list. In general, you should choose the detail view, if you are interested in more properties of the RFC calls logged by UCON because you need more information to analyze the incoming RFC calls.

The detail view contains the following additional fields:

- *Destination* (name of the destination, by which the RFC has been called)
- *RFC Server Client* (client, in which the RFM has been called)
- *RFC Server User* (user on server side)
- *Virtual Host* (Virtual host, by which the incoming call has reached the server system)
- *Rejected* (Has the call been rejected)
- *RFC Caller SID* (SID of calling system, if it is an ABAP-based system)
- *RFC Caller Client* (client, from which the RFM has been called)
- *Host* (of calling system, which is relevant, if the RFC has been called via an RFC-based connector)