How to Make Your RFC Connections More Secure in a Simple Way

**UCON RFC Basic Scenario**

Guide to Setup and Operations for 740 SP5 (and higher)

Version 1.0 | July 2014 | Dr. Thomas Weiss SAP SE

For more material on UCON see SCN: [http://scn.sap.com/docs/DOC-53844](http://scn.sap.com/docs/DOC-53844)
© Copyright 2014 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE and its affiliated companies (“SAP Group”) for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE in Germany and other countries. Please see http://www.sap.com/corporate-en/legal/copyright/index.epx#trademark for additional trademark information and notices.

This tutorial intends to complement SAP product documentation. While specific product features and procedures typically are explained in a practical business context, it is not implied that those features and procedures are the only approach in solving a specific business problem using SAP NetWeaver. Should you wish to receive additional information, clarification or support, please refer to SAP Consulting.

Any software coding and/or code lines / strings (“Code”) included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, except if such damages were caused by SAP intentionally or grossly negligent.

Disclaimer:
Some components of this product are based on Java™. Any code change in these components may cause unpredictable and severe malfunctions and is therefore expressly prohibited, as is any decompilation of these components.

Any Java™ Source Code delivered with this product is only to be used by SAP’s Support Services and may not be modified or altered in any way.
Table of Contents

How to Use this Guide ........................................................................................................................4
UCON RFC Basic Introduction and Overview .......................................................................................5
   The Way UCON RFC Basic Works in a Nutshell .................................................................................5
UCON RFC Basic Security and How to Achieve it ...............................................................................6
   General Pattern of Activities Required for UCON Security (for more details go to section
   “How to Set up and Configure the Different UCON Scenarios”) .......................................................6
   Life-Cycle-Management Enablement of UCON .............................................................................6
UCON RFC Basic Security – Activation and Operations on One Page .............................................9
The Different Ways to Work With the UCON RFC Basic Scenario ....................................................10
Authorizations for UCON RFC Basic ...............................................................................................11
Data Privacy Protection (as of 7.40 SP8) ..........................................................................................11
How to Set up and Configure UCON RFC Basic ................................................................................12
   A/B Productive and Test Use of UCON RFC Basic Scenario Local ....................................................12
   C UCON RFC Basic Scenario Landscape ......................................................................................14
   D UCON RFC for Logging Only .......................................................................................................17
   E Completely Deactivating UCON RFC Basic .................................................................................18
   F The Different Use Cases of the UCON RFC Basic Scenario in a Nutshell .....................................19
Operations of UCON RFC Basic .......................................................................................................20
   A/B Productive and Test Use of UCON RFC Basic Scenario Local ....................................................20
   C UCON RFC Basic Scenario Landscape ......................................................................................22
   D UCON RFC for Logging Only .......................................................................................................27
FAQ ................................................................................................................................................28
   What about New Scenarios, Which Need Might Need Access to RFMs that Are Already
   Blocked by UCON? ............................................................................................................................28
How to Use this Guide

This section tells you which kind of information this guide offers and how to find what you want to know.

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.

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 many customers want to protect PROD, but are not allowed to or do not want to execute the UCON operations in PROD, but prefer to define in DEV which RFMs they want to expose and which to block – based on RFC logging data from PROD –, and then to transport these definitions from DEV to PROD.

To get a deeper understanding of the basic concepts of UCON have a look at the SAP Insider article "SAP Insider: Secure Your System Communications with Unified Connectivity".

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".
UCON RFC Basic Introduction and Overview

The Way UCON RFC Basic Works in a Nutshell

UCON RFC is a framework 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 accessed from other systems or other clients in your business and technical scenarios.
b) Make the decision on which RFMs 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:

<table>
<thead>
<tr>
<th>Two-phase logging of incoming external RFC calls with the UCON Phase Tool</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Logging Phase:</strong> Find out which RFMs are called from outside in the system to be protected.</td>
</tr>
</tbody>
</table>

End of logging phase (indicated by a CCMS warning and the UCON Phase Tool):
Expose all RFMs that have been called during the logging phase by assigning them to a dedicated container called default Communication Assembly (CA).

| Evaluation Phase: Find out whether you have forgotten to expose any RFMs. |

End of Evaluation Phase (indicated by a CCMS warning and the Phase Tool):
Expose all RFMs that have been called during the evaluation phase and that are not yet assigned to the default CA.

UCON RFC basic security/protection for RFMs

| Final/check-active phase: Active UCON Runtime checks |

Final/check-active phase is open-ended:
- Only the RFMs exposed/assigned to the default CA are accessible from outside.
- The external access to all other RFMs (not assigned to the default CA) is blocked. Each attempt to reach an RFM blocked by UCON checks terminates the session on the server side, leads to a system log entry (SM21), and is indicated by a CCMS error.
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:

1. Create the UCON profile parameter and set it to 1.
2. Schedule the UCON batch job so that all incoming RFC calls from outside are logged and persisted.
3. Define the duration of logging and evaluation phase, then run the UCON setup: Create some technical entities needed for the operations of this UCON scenario and determine in which clients the UCON RFC protection should work.

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 SPs or EhPs, by upgrade, or by creation within the system.

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 cover the needs caused by the fact that most ABAP-based systems are part of a landscape and that, in general, not all administrative activities are allowed in PROD-systems: This is why the UCON operations have to be relocated to DEV even if you want to protect PROD based on the RFC logging data collected in PROD.
**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 are created in or arrive in the system by transports, installation of SPs or EhPs, 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. At the end of the initial UCON security classification, when all these RFMs have reached the final phase, they are all classified as either exposed or blocked for external access.

**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 it to the logging or evaluation phase.

**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: 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 them 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, many development or 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.

**General Rule of UCON: No Implicit Changes to the Security State of RFMs**

Security is essential to your systems, and you want 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. There is no such automatism because it is you who should always have full control of which RFMs are protected/block for external access and which are exposed by UCON.

**There is a deliberate exception to this general rule if you explicitly choose “Security by Default”:**

If you explicitly select the feature “Security by Default” (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 and are thereby blocked.

The point of SBD is to cover the following situation: You are in situation in which all RFMs needed for your connectivity scenarios are exposed and all other RFMs are blocked. You are sure that during the next months 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 are automatically blocked for external access by UCON SBD.
Activation of UCON RFC Basic:

1. Create the UCON RFC profile parameter and set it to 1.
2. Schedule the batch job to aggregate and persist the relevant RFC logging data.
3. Define the duration of logging and evaluation phase and run the UCON setup.

Initial UCON RFC Security Classification:

- Use the RFC logging data to find out which RFMs you need to expose (logging phase).
- Check whether you have forgotten to expose any RFMs you need for your business or technology/administrative scenarios and expose them also (evaluation phase).
- Block the access to all other RFMs (that you have not exposed) by assigning all RFMs in your system to the final phase and profit from UCON RFC protection.

Recurrent UCON RFC Security Operations:

A. **Classification of RFMs that are new in the system** (either created there or imported into the system): Expose the new RFMs in the system based on the RFC logging data analogous to the initial UCON security classification and protect the relevant RFMs once they have reached the final phase.

B. **Re-Assessment of called RFMs that were blocked by UCON**, that is of all RFMs that were called from outside, that are in the final/check-active phase and that did not pass the UCON runtime checks: Make up your mind as to whether the outside access to these RFMs is correctly blocked, whether you should expose them, or whether you need additional logging data to decide this.

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]).
The 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 only 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 practical experience with UCON for some time and want to easily deactivate it after this. As far as operations are concerned, there is no principal 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](#).

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 for UCON RFC Basic

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

The authorization needed for the UCON standard batch job is described in note 2044302. 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 Æ 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 the 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 are gone 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 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" whether this is explicitly mentioned or not.

3. 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 “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.

You can also use this window for a 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 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 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 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.

<table>
<thead>
<tr>
<th>PROD</th>
<th>DEV</th>
</tr>
</thead>
<tbody>
<tr>
<td>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)</td>
<td></td>
</tr>
<tr>
<td>Note: Always make sure that the profile parameter &quot;ucon/rfc/active&quot; has the same value on each server.</td>
<td></td>
</tr>
<tr>
<td>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).</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>
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).

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 Æ 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.
3. 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.

Note:
UCON logging starts after you have scheduled this batch job.

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

Assign the default CA, the VHs and configurations (both are client-dependent entities), and the state objects (they carry the information about the phase-assignments of the RFMs) to transport requests so that you can complete the UCON setup.

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

5. Release the transports with default CA, VHs and configurations, and state objects.

Note:
If you change the duration of the logging or evaluation phase 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.

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.

Note:
If you change the duration of the logging or evaluation phase 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.
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.

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.
   - Select “Transport of State Objects”. Press the Setup button at the bottom of the window.

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.

   **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.

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" 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 [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.

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

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Scope of Use Case</th>
<th>Value of UCON Profile Parameter (UCON/RFC/ACTIVE)</th>
<th>UCON Runtime Checks</th>
<th>Configure Default CA, Def. Host and Def. Conf. in at Least One Client</th>
<th>Schedule UCON Batch Job</th>
<th>Logging of External RFC Calls</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Productive use of RFC basic scenario local</td>
<td>Runtime checks, logging of RFC calls, and phase- and CA-assignment in one system for permanent use</td>
<td>1 (default parameter in RZ10 recommended, system restart required)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>B. Test use of RFC basic scenario local</td>
<td>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</td>
<td>1 (temporary parameter in RZ11 recommended, no system restart required)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>C1. PROD System part of RFC basic scenario landscape</td>
<td>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)</td>
<td>1 (default parameter in RZ10 recommended, system restart required)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>C2 DEV System part of RFC basic scenario landscape:</td>
<td>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)</td>
<td>0 (default parameter in RZ10 recommended, system restart required)</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>D Logging only</td>
<td>No runtime checks, logging of RFC calls, no phase- and CA-assignments (Two different ways to configure and set up this use case)</td>
<td>0 (default parameter in RZ10 recommended, system restart required)</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>UCON RFC completely switched off</td>
<td>No UCON entities at all, no runtime checks</td>
<td>0 (default parameter in RZ10 recommended, system restart required)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
**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 the 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.

**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. (These 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 fastest 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: 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: 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 the 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 process steps are performed once until all RFMs that are in your system at a given time are classified as exposed or blocked by UCON):

<table>
<thead>
<tr>
<th>PROD</th>
<th>DEV</th>
</tr>
</thead>
<tbody>
<tr>
<td>After the UCON setup the RFMs in a system are automatically assigned to the logging phase.</td>
<td></td>
</tr>
<tr>
<td><strong>Activities at the end of the logging phase:</strong></td>
<td></td>
</tr>
<tr>
<td>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”:</td>
<td></td>
</tr>
<tr>
<td>When a group of RFMs has reached the end of the logging phase you get a warning.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>PROD</td>
<td>DEV</td>
</tr>
<tr>
<td>------</td>
<td>-----</td>
</tr>
<tr>
<td>In the UCON Phase Tool (transaction UCONCOCKPIT or transaction UCONPHTL for releases lower than 740 SP7) under the header &quot;Use Statistics from System&quot; choose the SID of your PROD-system. This way the Phase Tool will show a selection from the RFC logging data of PROD.</td>
<td>Select &quot;Display RFMs with status 'expired' only&quot; (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.</td>
</tr>
<tr>
<td>Next you have two options:</td>
<td>Next you have two options:</td>
</tr>
<tr>
<td>• 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.</td>
<td>• 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.</td>
</tr>
<tr>
<td>Assign all selected RFMs to the def. CA and choose a transport request for the CA before saving your changes.</td>
<td>Assign all selected RFMs to the def. CA and choose a transport request for the CA before saving your changes.</td>
</tr>
<tr>
<td>Navigate back to the selection screen and select &quot;Function Modules in logging phase&quot;. (The property “Display RFMs with status ‘expired’ only” should still be selected.)</td>
<td>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).</td>
</tr>
</tbody>
</table>

**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.

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.
### 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 SP5 or higher, transaction UCONPHTL) and choose in the menu: Operations → Statistical Records → Export Statistics Records to save the RFC logging data to a file.

<table>
<thead>
<tr>
<th>PROD</th>
<th>DEV</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>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.</td>
</tr>
</tbody>
</table>
| 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. |
<p>| Assign all marked RFMs to the default CA.       |                                               |</p>
<table>
<thead>
<tr>
<th>PROD</th>
<th>DEV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate back to the selection screen and select &quot;Function Modules in evaluation phase&quot;. (The property &quot;Display RFMs with status 'expired' only&quot; should still be selected.)</td>
<td>Assign all RFMs to the final phase and choose a transport request for them.</td>
</tr>
</tbody>
</table>

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 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 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:
     o 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.
     o 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 the 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 fastest 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

What about New Scenarios, Which Need 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
- 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 at 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.