# Configure Cisco DCM – Remote Authentication Support

## Contents



## Introduction

This document describes the Cisco Digital Content Manager (DCM) softwareRemote Authentication using RADIUS.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of Cisco DCM software version 16 and above.

### Components Used

The information in this document is based on these software versions:

- Cisco DCM software v16.10 and above.
- RADIUS Server running with freeRadius open source software.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Background Information

In V16.10 of the DCM a new feature has been introduced that allows user accounts configured on a RADIUS server to be used to access the DCM GUI.This document describes the setup required

on the DCM and the RADIUS server to make use of this feature.

## GUI Accounts on DCM

In versions 16.0 and below the user accounts required to access the GUI were local to the DCM, i.e. created, modified, used and deleted on the DCM.

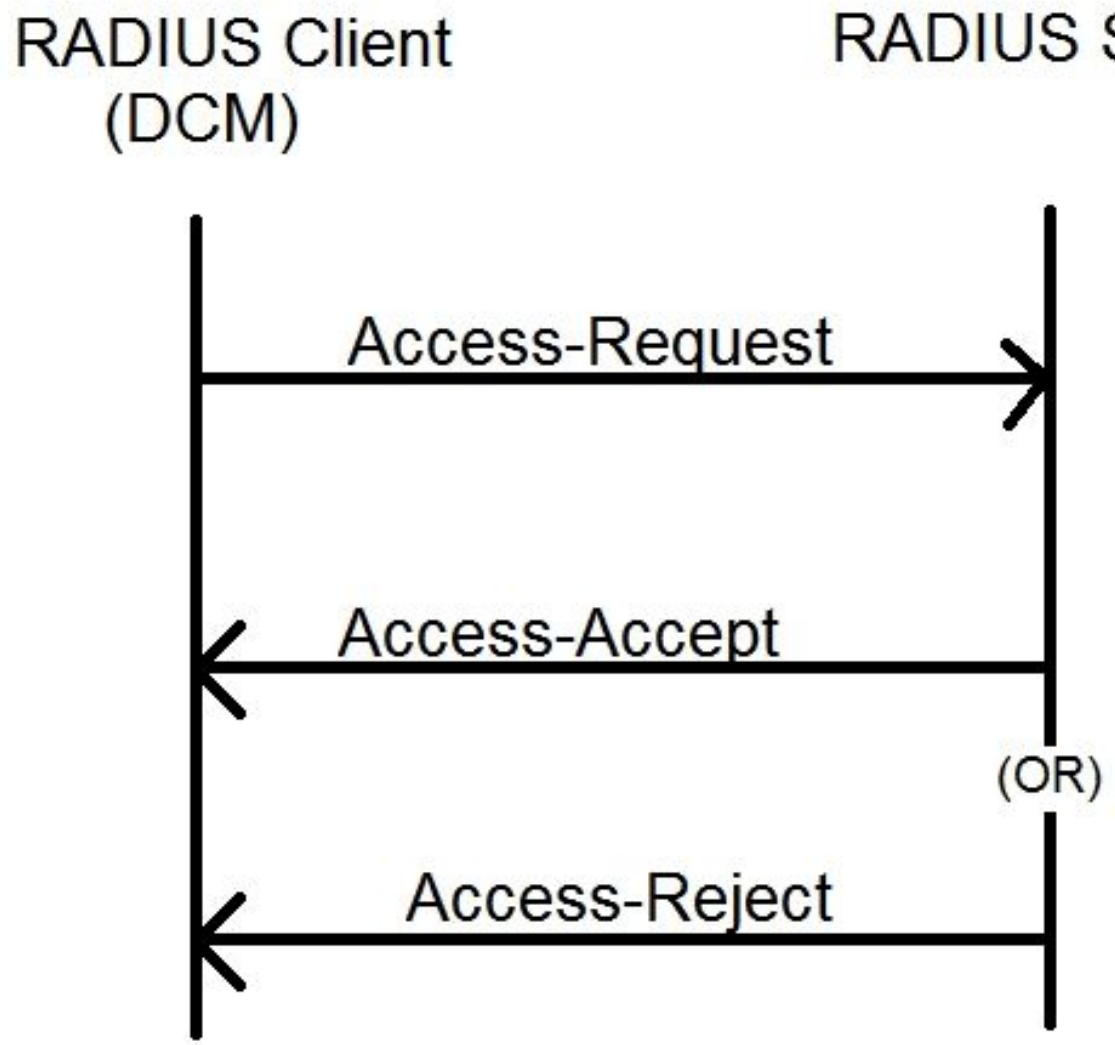
A GUI user account can belong to one of these groups:

- Administrators (Full Control)
- Users (Read-Write)
- Guests (Read Only)
- Automation triggers (External Triggers)
- DTF Administrators (DTF Key configuration)

## Remote Authentication

The idea of remote authentication is to have a centralized collection of user accounts which can be used to access a device, application, service etc.

The steps shown in the image explains what happens when you use remote authentication:




Step 1. User enters the login and password (user account configured on RADIUS server) on the login page on the DCM GUI.

Step 2. The DCM sends an Access-Request message with the credentials to the RADIUS server.

Step 3. The RADIUS server checks if the request has come from one of the configured clients and for the existence of the user account on its DB/File and validates if the password is correct or not, after which any one of the following messages are returned to the DCM

- Access-Accept – This means that the credentials are valid. The configured RADIUS attributes are returned.
- Access-Reject – This means that the credentials are invalid and the RADIUS server may be configured to send some RADIUS attributes to inform the failure.
- Access-Challenge – This means that the RADIUS server needs some additional information for validating the user's authenticity. Not processed in the DCM.

In case RADIUS server sends an Access-Reject, the DCM checks if the user account is local to the DCM itself and authentication procedure for that is followed.
The user is re-authenticated at an interval of 15 minutes (internally) to confirm that the

username/password is still valid and the user belongs to one of the GUI account groups. If the authentication fails the current running user session is deemed invalid and all the privileges are revoked for the user.

# Configure RADIUS Server

To use the user accounts present on RADIUS server for accessing the GUI these steps need to be followed:

DCM should be configured as a client to the RADIUS server.

1. Add the IP of the DCM as a client for the RADIUS server.
2. Add the shared secret to the client configuration (this shared secret should be the same as the one configured on the DCM, see section Configuring the DCM).
3. It is recommended to have a different shared secret for each DCM.
4. The length of the shared secret should be at least 22 characters long.
5. The shared secret should be as random as possible.

   Example of a good shared secret : ‘89w%$w*78619ew8r4$7$6@q!9we#%^rnEWR@#QEws13&4^%sf54gsf4@!fg3sdf#@sdf$d3g44fg3%2s2345’

For an user account the Access-Accept message from the RADIUS server should have a RADIUS attribute which identifies the GUI account group to which the user belongs. The attribute name can be chosen and needs to be configured in the settings file on the DCM.

This is the format of the string that needs to be sent as a value for an attribute from the RADIUS server:

**OU=<group_name_string>** group_name_string can be one of these:

| **Group** | **Group name string** |
|---|---|
| Administrators (Full Control) | administrators |
| Users (Read-Write) | users |
| Guests (Read Only) | guests |
| Automation triggers (External Triggers) | automation |
| DTF Administrators (DTF Key configuration) | dtfadmins |

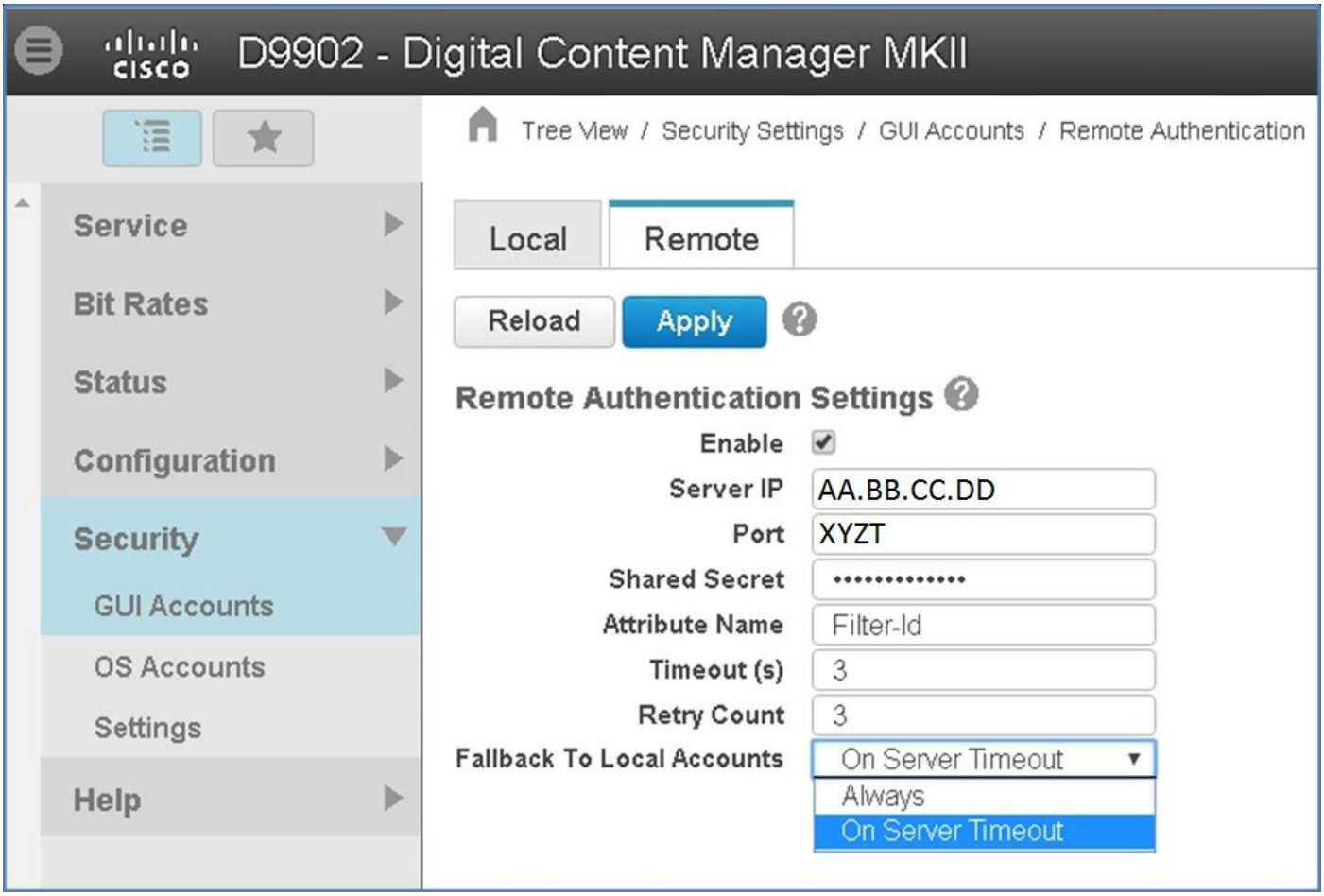
# Configure Cisco DCM

To enable/configure remote authentication feature on the DCM a GUI Administrator account is required.

These steps indicate how to configure remote authentication:

Step 1. Login to the DCM using Administrator account.

Step 2. Navigate to **Security > GUI Accounts** and select **Remote** tab, as shown in the image:




Step 3. Configure the parameters required for RADIUS communication:

- Enable - This setting determines if Remote authentication support should be enabled or not. When checked the rest of the parameter fields are enabled.
- Server IP - IP address of the RADIUS server.
- Port - Port on which the RADIUS server is listening for authentication packets (generally 1812 but can be configured to other values).
- Secret - This is the shared secret that is used to encrypt the password before sending the RADIUS packet to the server. This secret should be the same as that configured on the RADIUS server where it is used to decrypt the password.
- Attribute Name - The name of the attribute in which the authorization data is received from the RADIUS server.
- Timeout (in seconds) - This setting is used for communication between the RADIUS server and DCM. This is the time that the DCM should wait for a response from the RADIUS server

for a particular request before terminating the request.

- Retry Count - Number of times the RADIUS request must be sent in case previous requests are timed out.

- Fallback To Local Accounts - This setting is available from DCM version 19.0 onwards. The DCM allows to log on using a GUI (local) account that is created using the GUI. Option, **On Server Timeout** allows to fallback to the local accounts in case the Radius server cannot be reached, and not when authentication failed. Option, **Always** allows to fallback always – even when authentication failed.

Step 4. As the changes are applied the warning shown in the image is displayed. Click **OK** and the user interface is restarted.


Step 5. Now the DCM is ready for remote authentication.

Configure IPSec on DCM:

1. Log on to the DCM using a GUI account that belongs to the Administrators security group.

2. Navigate to **Configuration > System**. The System Settings page appears.

3. Refer to the **Add New IPsec** area, as shown in the image.


4. In the IP Address field, enter the IP address of the new IPsec peer (RADIUS server).

5. In the **Pre Shared** key and Retype *Pre Shared Key* fields, enter the *Pre Shared Key* for the new IPsec peer.

6. Click **Add**. The new IPsec peer is added to the IPsec Settings table.

> **Note**: For configuration of IPSec on the machine on which RADIUS server is running refer to the documentation/publication provided with the product.

# Security Considerations

- The shared secret is stored in the clear in the file system of the DCM.
- The encrypted password is stored in the memory of the DCM for use in re-authentication for the duration of the session.
- Given the two items above, it is advised to limit who has troubleshooting access to the DCM.
- It is strongly advised to use IPSec to secure the communication channel between DCM and RADIUS
  server.

# Constraints and Limitations

- The remote authentication support is only available for the GUI accounts, not for the OS accounts.
- A re-authentication is done at an interval of 15 minutes. Example: If a user's group has been changed, the worst case time taken for the change to take affect is 15 minutes.
- If remote authentication is enabled, the DCM first checks with the RADIUS server if the user account is valid or not and then checks on the local database. In case of using local accounts which do not exist on the RADIUS server there would be an authentication failure message on RADIUS server.

# Set up freeRadius

This section shows as an example how to setup freeRadius to use as remote authentication server for the DCM. This is for informational purposes only,

Cisco does not provide or support freeRadius. It is assumed that the configuration files for freeRadius are found under **/etc/freeRadius/** (check distribution).

After installing freeRadius package modify these files.

- Modify the **/etc/freeradius/clients.conf**
  Step 1. Add an entry for the IP of the DCM to the list of clients.

Step 2.Add the shared key in the client configuration and leave the other parameters to default.

It is recommended to have a unique shared secret for each DCM.
The length of the shared secret should be atleast 22 characters long. The shared secret should be as random as possible.

Example of a good shared secret :
‘89w%$w*78619ew8r4$7$6@q!9we#%^rnEWR@#QEws13&4^%sf54gsf4@!fg3sdf#@sdf$d3g44fg3%2s2345’

- Modify the **/etc/freeradius/radiusd.conf** to change the port on which the radius server should listen (generally 1812)

- Modify the **/etc/freeradius/users** to add new users.

- Ensure to add the RADIUS attribute in which authorization information is sent to the DCM in this format:
<Attribute Name> = '**OU=<group_name>'**

Attribute Name: This is the name of the standard RADIUS attribute on which the authorization data is sent to the DCM group_name can be one of the following:
administrators - A user that belongs to this group will have administrator privileges i.e. Full control.
users - A user that belongs to this group will have read-write privileges.
guests - A user that belongs to this group will have read only privilege.
automation - Used for automation (External triggers).
dtfadmins - DTF Administrator (DTF Key Configuration)

Example:
steve Cleartext-Password := "testing"
Filter-Id = "OU=administrators"

- (Re)start the radius server for the changes to take effect.

- Ensure that the firewall configuration of the radius server allows external access to the chosen port.

# Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

For debugging purposses some additional logs have been introduced into the Security Log. In order to view this log navigate to **Help > Traces page** in DCM GUI.

This section describes what to look for in the logs, what the issues could be and possible solutions.

| | |
|---|---|
| Log line | Remote login attempt failed: Request to the RADIUS server was timed out. |
| Issue | DCM is not able to communicate with the RADIUS server. |
| Possible Solution | • Verify that the RADIUS Server IP address provided in the remote authentication configuratio in the DCM is actually correct.<br>• Ensure that the RADIUS server is accessible from the DCM.<br>• Ensure that the DCM is configured as a valid client on the RADIUS server (RADIUS server silently drops Access-Request packets from unknown clients).<br>• Ensure that the shared secret configured on the DCM is the same as the shared secret configured on the RADIUS server for that particular DCM. (If the server does not possess a shared secret for the client, the request is silently dropped.) |
| Log line | Remote login attempt failed : [Errno 10054] An existing connection was forcibly closed by the re host. |
| Issue | The DCM has sent a RADIUS request to the specified Server IP. However, the RADIUS server application is not listening on the port specified in the remote authentication settings. |
| Possible Solution | • Ensure that the RADIUS server is running.<br>• Check that the Port number specified in the RADIUS configuration on the server is the sam the one configured on the DCM. |
| Log line | Remote login attempt failed: Invalid attribute name specified or response from RADIUS server missing authorization data. |
| Issue | There is a problem with the response received from the RADIUS server. |
| Possible Solution | • Ensure that the RADIUS server sends the attribute (configured on the DCM) in the ‘Access Accept’ response.<br>• Ensure that the **Attribute Name** parameter configured on the DCM remote authentication settings is the exact name as specified in the user configuration on the RADIUS server. |
| Log line | Invalid authorization data received from RADIUS Server. |
| Issue | Authentication succeeded but the response received from the RADIUS server contains invalid authorization data i.e. security group name. |
| Possible Solution | • Ensure that the group name configured on the RADIUS server for that user is one of the security group name specified in the section Configuring RADIUS Server.<br>• Ensure that the format of the string configured on the RADIUS server is according to the o specified in the section Configuring RADIUS Server. |