Оглавление

[Build 2](#_Toc437216012)

[Installation and configuration 2](#_Toc437216013)

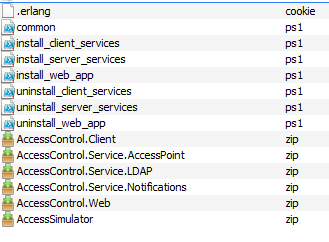
[How to configure daily reports 5](#_Toc437216014)

[Troubleshooting 9](#_Toc437216015)

[Feedback 9](#_Toc437216016)

# Build

1. **Run build\ClickToBuild.cmd**
2. **Goto Artifacts folder and ensure that the build contains the following files:**



# Installation and configuration

Prerequisites:

* Server Failover Cluster for hosting RabbitMQ and server-specific services
* MS SQL Server Failover Cluster
* Web Server or cluster of web servers with Network Load Balancing
* Client Failover Cluster for hosting client-specific services to which vendor software connects

1. **Install and configure RabbitMQ on each node**

The following steps should be executed for each node in your cluster.

* 1. Goto System -> Environment Variables and add RABBITMQ\_BASE system variable to point your cluster drive (for me it's F:\RabbitMQ). RabbitMQ uses this variable for creating databases and files. Do not pick a cluster disk!
  2. Download and install Erlang <http://www.erlang.org/download.html>
  3. Download and install RabbitMQ <https://www.rabbitmq.com/download.html>
  4. Copy and replace .erlang.cookie file from Artifacts folder to the locations:
* %SystemPath%\
* %SystemPath%\ServiceProfiles\NetworkService
* %SystemPath%\ServiceProfiles\LocalService
* Users\%CurrentUser%
  1. Open the following ports:
* 5672 This is the main AMQP port that clients use to talk to the broker.
* 15672 The management web interface.
* 4369 Used by EPMD (Erlang Port Mapper Daemon). This makes sure that the nodes can find each other.
  1. Allow connection for two binaries %Program Files%\erl7.1\bin\erl.exe and %Program Files%\erl7.1\erts-7.1\bin\erl.exe. This allows Erlang to communicate between nodes. Optionally you can configure allowed ports instead of erl.exe. For more details see RabbitMQ documentation.
  2. Run RabbitMQ Command prompt and enable execute the commands:
* rabbitmq-plugins.bat enable rabbitmq\_management
* rabbitmq-service.bat stop
* rabbitmq-service.bat install
* rabbitmq-service.bat start

1. **Create RabbitMQ cluster**

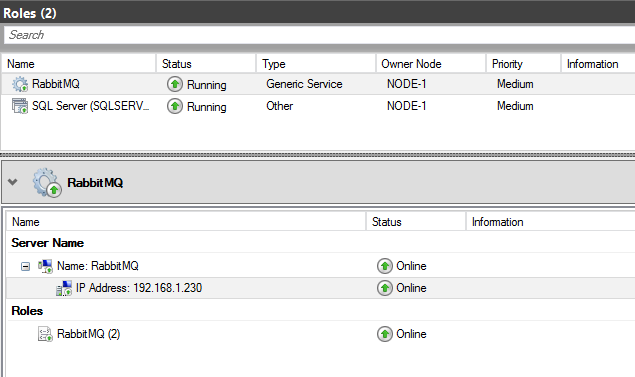
The next steps should be executed on a node of your cluster, which is considered by RabbitMQ as slave node (see RabbitMQ documentation for details)

* 1. Run RabbitMQ Command Prompt on your slave node and join the cluster and set mirroring policy:
* rabbitmqctl stop\_app
* rabbitmqctl join\_cluster rabbit@YOUR\_MASTER\_NODE
* rabbitmqctl start\_app
* rabbitmqctl set\_policy HA ".\*" "{""ha-mode"": ""all""}"

NOTE: YOUR\_MASTER\_NODE should be in UPPER CASE.

* 1. Delete guest access and add a new user, which will be used by services. Remember username/password to configure services later (by default “evgeny/Test123”).
* rabbitmqctl add\_user <username> <password>
* rabbitmqctl set\_permissions <username> ".\*" ".\*" ".\*"
* rabbitmqctl set\_user\_tags <username> management
* rabbitmqctl delete\_user guest

1. **Create a cluster role for RabbitMQ**
   1. Run Failover Cluster Manager and add a new Generic Service role
   2. Pick RabbitMQ service as a target service for the role
   3. Assign a new IP address for the RabbitMQ cluster role. Remember this address to configure services later (by default, 192.168.1.230).
   4. Bring RabbitMQ role online.

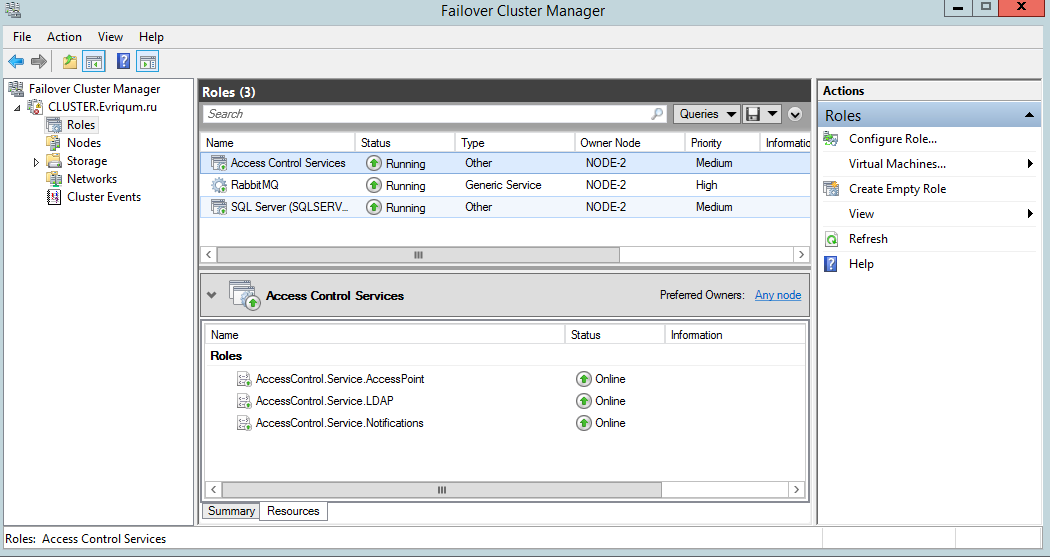


**Important note:** when you need to restart RabbitMQ cluster you should guarantee that node, which is last to go down should be first to go up. For details, see RabbitMQ documentation.

1. **Create a new database for access control system**
   1. Create a new empty MSSQL SERVER database. You should not create database schema, application will created schema automatically at first startup. (by default, database name is AccessControlSystem)
2. **Server services deployment**
   1. Copy files from artifacts folder on each node of your Server Cluster and run

install\_server\_services.ps1

* 1. Enter the information asked by the script
  2. Goto Services snap-in and ensure that the following services are installed:
* AccessControl.Service.LDAP
* AccessControl.Service.AccessPoint
* AccessControl.Service.Notifications
  1. Create a new cluster role named Access Control Services and add all services from the list above to this role as Generic Services.



* 1. Optional step: You can create a sample organizational structure automatically. To perform it, copy create\_ldap\_users.ps1 and import\_create\_ad\_users.csv to your LDAP server and run the script.

1. **Web application deployment**
   1. Copy files from artifacts folder to your Web Server and run install\_web\_app.ps1
   2. Enter the information asked by the script
   3. Run IIS and ensure that AccessControl.Web website is installed and configured
   4. In you have a cluster of web servers you should setup and configure Network Load Balancing for the port used by the AccessControl.Web website. By default, deployment script configures 8967 port. Failover cluster is not recommended for websites.
   5. Run a browser and navigate to <http://localhost:8967>. You should be able to login using your LDAP account and view users, user groups etc.
2. **Client services deployment**
   1. Copy files from artifacts folder to your Client Cluster server and run install\_client\_services.ps1
   2. Go to Services snap-in and ensure that AccessControl.Client service is installed
   3. Create a new cluster role named Access Control Client and add AccessControl.Client service to this role as Generic Service.

# How to configure daily reports

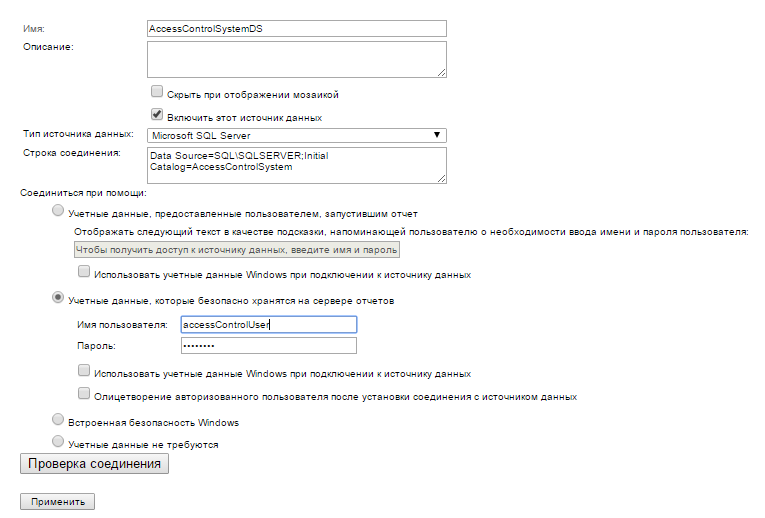
This section describes how to configure the system to create daily reports.

Before you start ensure that the database schema is generated (you need to run AccessControl.Web application and login)

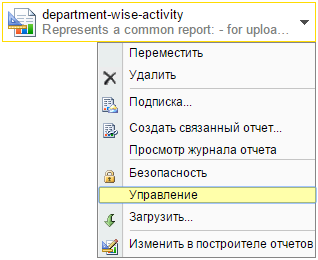
To proceed the steps below you need MSSQL Management Studio and MSSQL Reporting Services installed. Ensure that you properly configured SMTP for MSSQL Reporting Services to send emails.

Note: Sorry for language on the screenshots. I have only localized version of Reporting Services.

1. **Prepare database.**
   1. Run MSSQL Management Studio and open *reporting\report\_functions.sql* script.
   2. Replace values of *@AD\_UserName* and *@AD\_Password* variables with your Active Directory credentials.
   3. Execute the script
2. **Configure Report Manager**
   1. Open Report Manager web application.
   2. In Report Manager create a new data source and configure connection string to the database. This data source is going to be used for fetching report data.
   3. Click on Subscriptions and then create a new data-driven subscriptions.



* 1. From Report Manager run Report Builder and open *reporting\department-wise-activity.rdl* file.
  2. Add a server data source created earlier and upload that file on Report Manager.
  3. Locate the uploaded file and click Management in context menu and navigate to Subscriptions



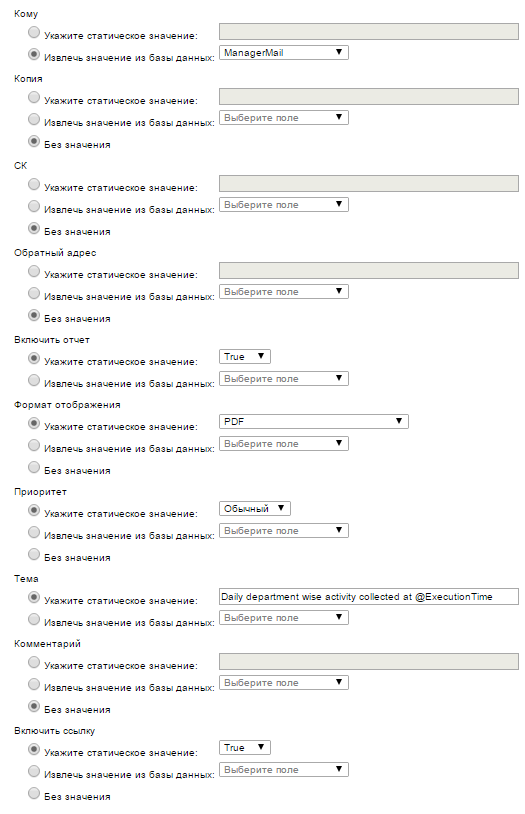
1. **Schedule daily department-wise activity log mailed to managers.**
   1. Create a new data-driven subscription.
   2. Enter description: Mailing to the department managers
   3. Use the data source AccessControlSystemDS created earlier
   4. Enter the following query to execute:

*DECLARE @domain VARCHAR(100) = '<domain name, for instance, evriqum.ru>'*

*DECLARE @dayOffset INT = 0 -- current day*

*EXEC dbo.ListDayLogTargets @domain, @dayOffset*

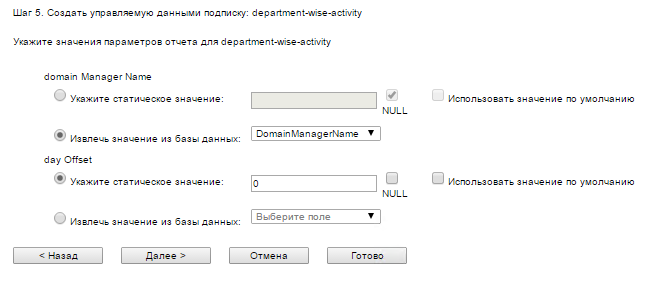
* 1. Specify values: sender – ManagerMail, Attach report – True, Format - PDF



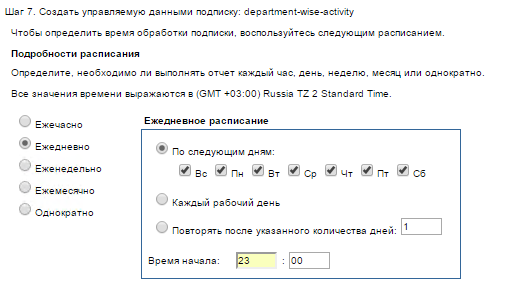
* 1. Enter report parameter values:

@domainManagerName = DomainManagerName from DB

@dayOffset = 0



* 1. Create a new schedule for the subscription



* 1. Click Finish

1. **Schedule department-wise attendance log uploaded as CSV into a shared folder.**
   1. Create a new data-driven subscription.
   2. Enter description: Uploading to a shared folder
   3. Use the data source AccessControlSystemDS created earlier
   4. Enter the following query to execute:

*DECLARE @domain VARCHAR(100) = '<domain name, for instance, evriqum.ru>'*

*DECLARE @dayOffset INT = 0 -- current day*

*EXEC dbo.ListDayLogTargets @domain, @dayOffset*

* 1. Specify deployment values

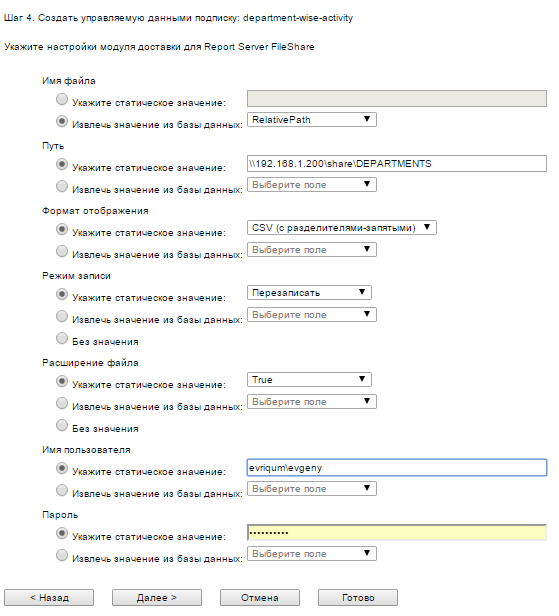
File name – RelativePath from database

Path – absolute path to a shared folder

Format – CSV

Mode - Overwrite

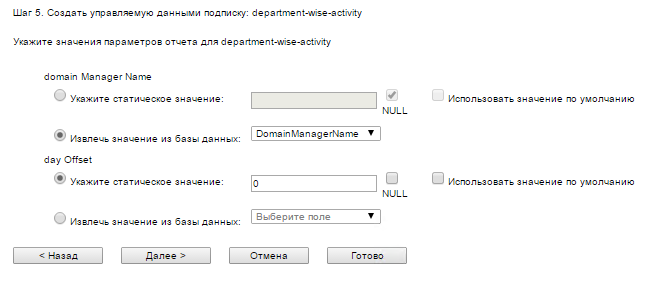
Your credentials to access the specified shared folder



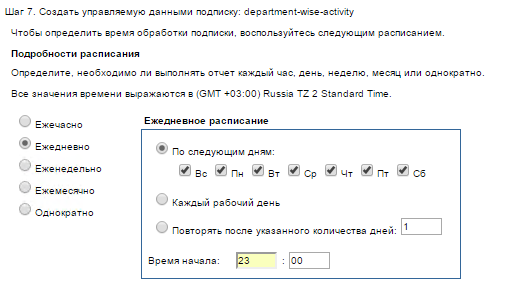
* 1. Specify report parameter values:

@domainManagerName = DomainManagerName from database

@dayOffset = 0



* 1. Create a new schedule for the subscription



* 1. Click Finish

# Troubleshooting

* 1. In case of problems with WCF services, when Windows blocks an URL because it is not added to the access control list, execute the following commands:
* netsh http add urlacl url=http://+:9981/AccessCheckService user=<your user name>
* netsh http add urlacl url=http://+:9981/AccessPointRegistry user=<your user name>
  1. If you have a problem with IIS and ASP.NET 4.5. Execute the following command
* dism /online /enable-feature /all /featurename:IIS-ASPNET45

# Feedback

I found many black spots in the specification.

1. I assume that user names remains read-only because LDAP directory does allow changing it.
2. I did not find any specification of 3rd party API exposed by vendor software. So I assumed that vendor API defines a WCF contract
3. I did not find any requirements to management system of access points but managers should do it. Therefore, I assumed that manager is responsible for management of access points located in his department.
4. Because of Internet can be switched off unexpectedly, we should guarantee that employees allow access points. However, there are no requirements, which would say if the system should guarantee notification delivery. If it is required, the client service should store such notifications in internal databases or in files and deliver then when connection is established. At this point, this implementation is out of the scope of the task.
5. There are no security requirements. I believe that the system should support Single Sign-On, therefore, I have created a simple implementation. System creates an encrypted ticket and passes it to remote services.
6. The system should communicate using SSL, to protect data from unauthorized access.
7. I did not find any requirements, which would describe how system handles electricity issues. Therefore, I assumed that 3rd party vendor hardware is responsible for it.