RSA

GUC
German University in Cairo

# (NETW 1002)

# Systems and Network Security

# Milestone 2

## Deadline: Thursday, 1 May 2025

OWN YOUR IDENTITY.

# Milestone 2:

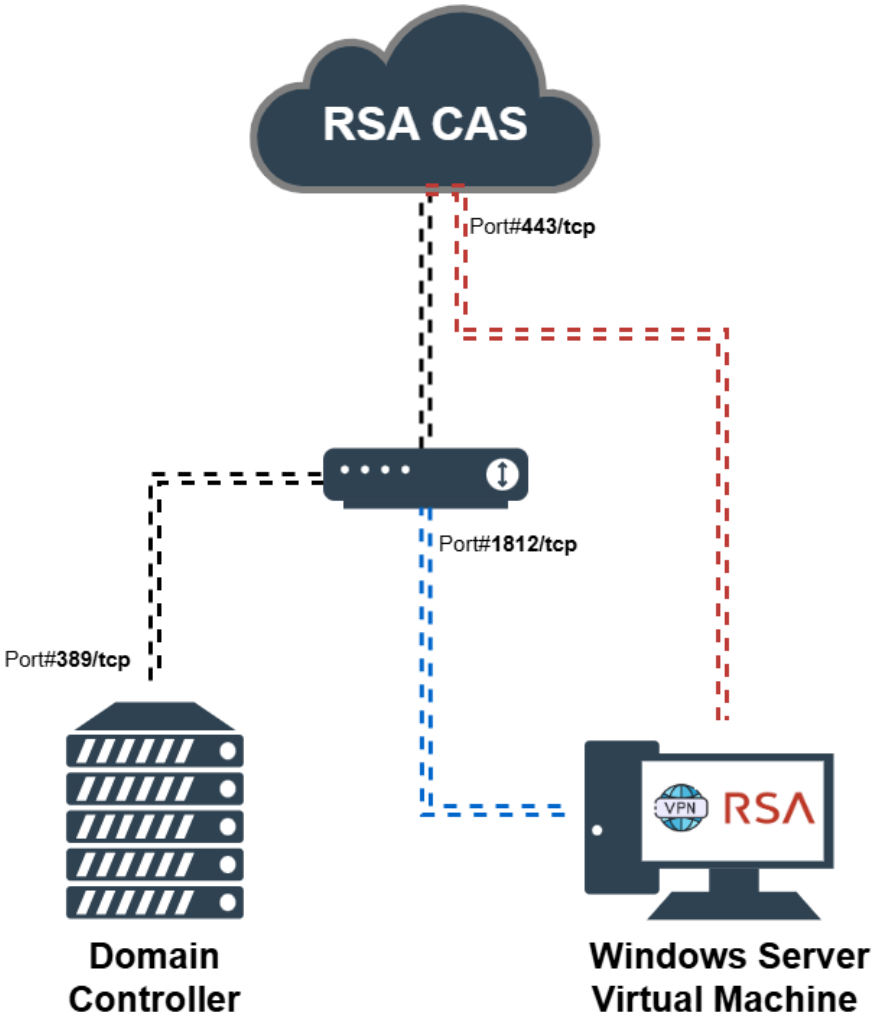
1. **Install a Windows Server virtual machine for RSA MFA deployment.**
    a. Add a static IP address to this Windows machine and add the IP address of the AD Windows machine as a DNS server for this machine.
    b. Connect this machine to the domain controller.

2. **Protect the Windows Virtual Machine with RSA MFA Agent**
    a. Download the latest RSA MFA Agent as a zipped file
    b. Copy and paste the RSA MFA Agent for Windows zipped file on the Windows virtual machine.
    c. Unzip the RSA MFA Agent for Windows zipped file.
    d. Execute RSA MFA Agent for Microsoft Windows x64
    e. Configure the RSA MFA Agent for Windows
        I. From the RSA CAS side
            1. Add a 1.0 access policy called **MFA Policy** that enforces multi-factor authentication utilizing a notification-based challenge for user verification.
            2. Copy the authentication API REST URL
            3. Add an API Access Key and copy it into a notepad.
        II. From the RSA MFA Agent side
            1. Open the start menu > Write "Edit Group Policy"
            2. Choose Local Computer Policy > Computer Configuration > Administrative Templates > RSA Desktop.
                a. In the Local Authentication Settings folder, enable and configure the following policies with the appropriate entries
                    i. RSA Challenge Group
                    ii. Specify the format used when sending usernames to the RSA authentication server during an MFA authentication
                    iii. Specify logging options
                        1. Set the log level to **VERBOSE**.
                        2. Select all the components to include in the log files
                    iv. Enable offline authentication
                b. In the RSA Settings folder, enable and configure the following policies with the appropriate entries
                    i. RSA Authentication API Key
                    ii. Cloud Authentication Service access policy
                    iii. RSA Authentication API REST URL
            3. Open the start menu > Execute "RSA MFA Agent Test Authentication" as an administrator
            4. Enter a username for a user who is a member of the challenge group
            5. You should be prompted to additional authentication using the push notification method
            6. You should have received a push notification on the RSA Authenticator App
            7. After approving the challenge request, a successful authentication method should be promoted
    f. Validate the user authentication activity from the CAS User Event Monitor.
    g. Make sure that offline days are downloaded from the RSA CAS User Event Monitor.
    h. Make sure that offline days are downloaded in the offline days folder on Windows VM
    i. Do an offline authentication by entering the authenticate tokecode.
    j. When 'Testing online and offline authentication' shows SUCCESSFUL, navigate to ***Local Group Policy Editor > Local Computer Policy > Computer Configuration > Administrative Templates > RSA Desktop > Local Authentication Settings*** and make sure that **the Enable RSA authentication group policy** is enabled.

k. Lockout your PC and try to authenticate using the test user
    I. You should be prompted to enter the LDAP user password and then receive a push notification for the additional authentication.

3. **Integrate a RADIUS client with RSA CAS**
    a. Download the latest NTRADPing as a zipped file
    b. Add a RADIUS client on RSA CAS and configure it so that:
        I. Cloud Authentication Service validates both passwords and applies an access policy for additional authentication.
        II. Challenged users will always be authenticated using push notification
        III. The code-matching feature should be disabled. Hint, make sure that Strict code-matching enforcement is disabled
        IV. Set the same access policy used in the RSA MFA Agent configurations
    c. Transfer the zipped file to the Windows machine on which the RSA MFA Agent is installed
    d. Extract the zipped file and open the NTRADPing program
    e. Check the User Event Monitor for the authentication attempt

## Expected Architecture:



**Reference Links:**

1. Assurance Levels & Configure Assurance Levels
2. Access Policies, Manage Access Policies & Access Policy Examples
3. Manage the RSA Authentication API Keys
4. Add a RADIUS Client for the Cloud Authentication Service
5. Configure Code Matching Settings