



(NETW 1002)

# Systems and Network Security

## Milestone 2 Submission Report

OWN YOUR  
IDENTITY.

## Milestone 2 Report Submission:

### Virtual Machines Network Settings:

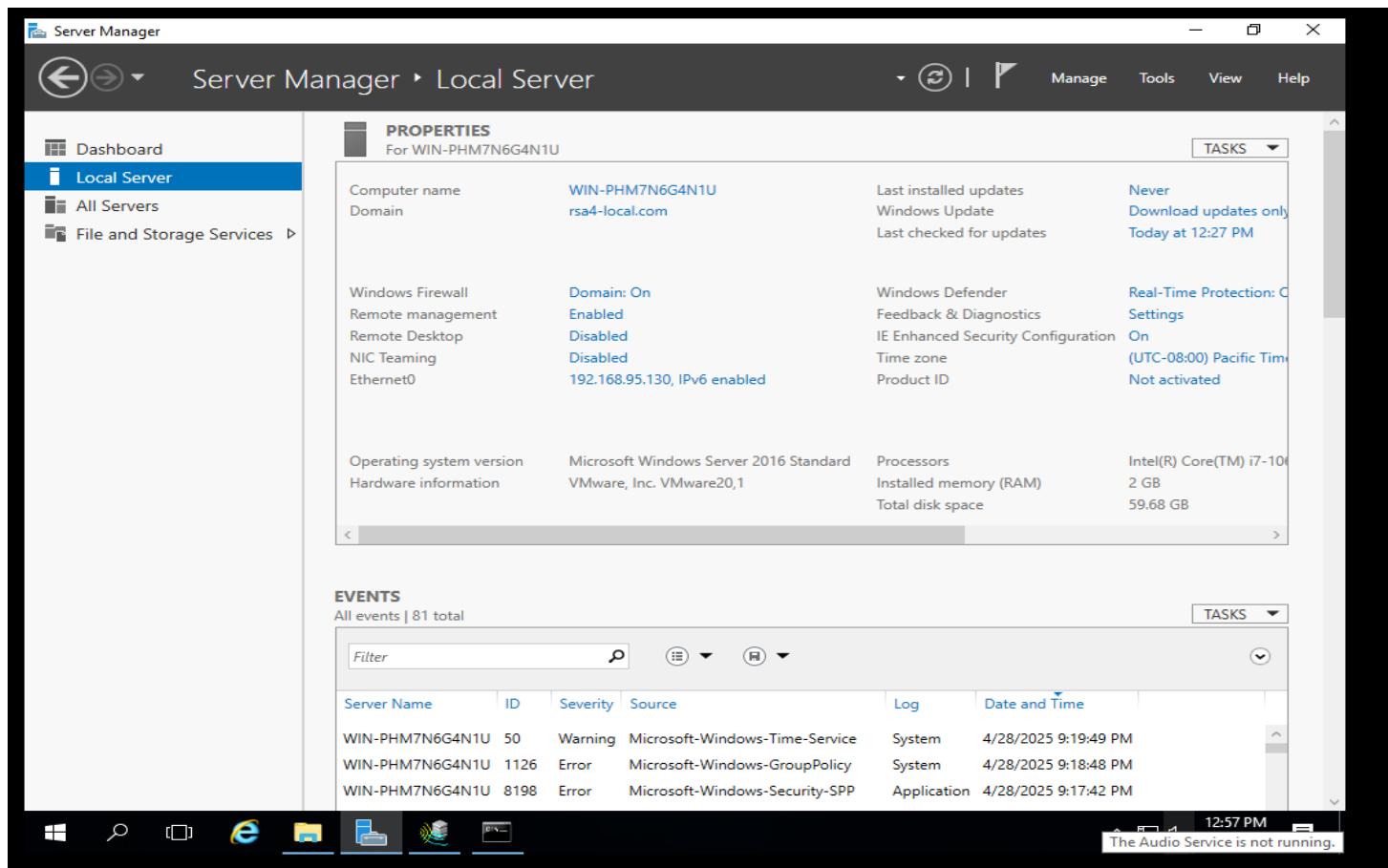
- Virtual Machine #3:

Virtual Machine Function (Domain Controller/MFA Agent/IDR)	MFA Agent
Operating System (Windows/Linux)	Windows
Fully Qualified Domain Name	rsa4-local.com
IP Address	192.168.95.130
Gateway	192.168.95.2
DNS	Primary:192.168.95.128 Secondary:8.8.8.8

## Milestone 2 Screenshots:

### 1. Windows Server virtual machine Installation

\*\*\* FIRST SCREENSHOT: Take a full-page screenshot of the Server Manager > Local Server



### 2. RSA MFA Agent Configuration

#### a. Policies applied locally on Windows VM

- Open PowerShell as administrator
- Execute the following command: `gpresult /user administrator /scope computer /h c:\Users\Administrator\Desktop\gpo.html /f`

*Note: The username: Administrator could be any other username based on the administrator managing this PC*

**Group Policy Results**

RSA4-LOCAL\WIN-PHM7N6G4N1U  
Data collected on: 4/28/2025 1:01:03 PM

### Summary

During last computer policy refresh on 4/28/2025 12:22:08 PM
<span style="color: green;">✓</span> No Errors Detected
<span style="color: yellow;">⚠</span> A fast link was detected <a href="#">More information...</a>
No data available.

### Computer Details

#### General

Computer name	RSA4-LOCAL\WIN-PHM7N6G4N1U
Domain	rsa4-local.com
Site	Default-First-Site-Name
Security Group Membership	<a href="#">show</a>

### Component Status

Component Name	Status	Time Taken	Last Process Time	Event Log
Group Policy Infrastructure	Success	539 Millisecond(s)	4/28/2025 12:22:08 PM	<a href="#">View Log</a>
Registry	Success	94 Millisecond(s)	4/28/2025 12:03:52 PM	<a href="#">View Log</a>
Security	Success	297 Millisecond(s)	4/25/2025 10:37:43 AM	<a href="#">View Log</a>

### Settings

#### Policies

- Windows Settings
- Security Settings
- Account Policies/Password Policy

**Account Policies/Password Policy**

Policy	Setting	Winning GPO
Enforce password history	24 passwords remembered	Default Domain Policy
Maximum password age	42 days	Default Domain Policy
Minimum password age	1 days	Default Domain Policy
Minimum password length	7 characters	Default Domain Policy
Password must meet complexity requirements	Enabled	Default Domain Policy
Store passwords using reversible encryption	Disabled	Default Domain Policy

**Account Policies/Account Lockout Policy**

Policy	Setting	Winning GPO
Account lockout threshold	0 invalid logon attempts	Default Domain Policy

**Local Policies/Security Options**

**Network Access**

Policy	Setting	Winning GPO
Network access: Allow anonymous SID/Name translation	Disabled	Default Domain Policy

**Network Security**

Policy	Setting	Winning GPO
Network security: Do not store LAN Manager hash value on next password change	Enabled	Default Domain Policy
Network security: Force logoff when logon hours expire	Disabled	Default Domain Policy

**Public Key Policies/Certificate Services Client - Auto-Enrollment Settings**

Policy	Setting	Winning GPO
Automatic certificate management	Enabled	[Default setting]
Option	Setting	
Enroll new certificates, renew expired certificates, process pending certificate requests and remove revoked certificates	Disabled	
Update and manage certificates that use certificate templates from Active Directory	Disabled	

RSA Desktop/Local Authentication Settings		
Policy	Setting	Winning GPO
Enable offline authentication	Enabled	Local Group Policy
RSA Challenge Group	Enabled	Local Group Policy
<p>Select the users to challenge</p> <p>Challenge: <input type="text"/> Users In a group</p> <p>Enter the name of the challenge group in the format &lt;domain name or machine name&gt;\&lt;group name&gt;.</p> <p>For example: CORP\SecurID Users</p> <p>Group name: <input type="text"/> rsa4-local\Project</p> <p>Secondary Group name:</p>		
Policy	Setting	Winning GPO
Specify logging options	Enabled	Local Group Policy
<p>Select the log level. <input type="text"/> Verbose</p> <p>Select the number of log files to rotate. <input type="text"/> 5</p> <p>Select the log file size. <input type="text"/> 5 MB</p> <p>Enter the path to store log files. <input type="text"/></p> <p>Select the components to include in the log files.</p> <ul style="list-style-type: none"> <li>OfflineAuthentication <input type="checkbox"/> Enabled</li> <li>RsaMfaAgentTestAuthentication <input type="checkbox"/> Enabled</li> <li>SIDAccessCredentialProvider <input type="checkbox"/> Enabled</li> <li>SIDAccessNotificationIcon <input type="checkbox"/> Enabled</li> <li>SIDAccessPasswordLessCredentialProvider <input type="checkbox"/> Enabled</li> </ul>		
Policy	Setting	Winning GPO
Specify the user name format sent to the RSA authentication server	Enabled	Local Group Policy
<p>Specify the User Name Format.</p> <p>Format: <input type="text"/> UPN</p> <p>Specify Excluded Domains (optional)</p>		

C:\Users\Administrator\Desktop\gpo.html

SIDAccessPasswordLessCredentialProvider  Enabled

Policy	Setting	Winning GPO
Specify the user name format sent to the RSA authentication server	Enabled	Local Group Policy
<p>Specify the User Name Format.</p> <p>Format: <input type="text"/> UPN</p> <p>Specify Excluded Domains (optional)</p> <p>Domains:</p> <p>RSA recommends listing both the DNS and Windows NTLM domain name.</p> <p>For example, to exclude a domain with a DNS name of 'corp.domain.com' and a Windows NTLM name of 'CORP', enter the following:</p> <p>CORP.corp.domain.com</p>		

RSA Desktop/RSA Settings		
Policy	Setting	Winning GPO
Cloud Authentication Service Access Policy	Enabled	Local Group Policy
<p>Enter the exact name of the access policy as specified in the Cloud Administration Console.</p> <p>MFA Policy</p>		
Policy	Setting	Winning GPO
Enable RSA authentication	Enabled	Local Group Policy
RSA Authentication API Key	Enabled	Local Group Policy
<p>Enter the RSA Authentication API Key.</p> <p>75835c038a7a8ed775c16712504bc55ec4be77c0</p>		
Policy	Setting	Winning GPO
RSA Authentication API REST URL	Enabled	Local Group Policy
<p>Enter the RSA Authentication API REST URL.</p> <p>https://la4.auth-demo.securid.com:443/</p>		

## Policy Objects

## b. Configurations done on RSA CAS side

\*\*\* SECOND SCREENSHOTS: The configurations mentioned below

- Access Policy applied
- RSA Authentication API Key
- RSA Authentication API REST URL

### Access Policy applied

Status: Success ✓ Publish Changes

Home Users ▾ Access ▾ Applications ▾ Authentication Clients ▾ Platform ▾ Dashboards ▾ Help My Account ▾ Sign Out

#### MFA Policy

All fields are required (except where noted)

**Name and Description**

**Identity Sources**

**Primary Authentication**

**Rule Sets**

Name: MFA Policy

Description (optional): policy for MFA

Cancel Next Step

Status: Success ✓ Publish Changes

Home Users ▾ Access ▾ Applications ▾ Authentication Clients ▾ Platform ▾ Dashboards ▾ Help My Account ▾ Sign Out

#### MFA Policy

Select at least one identity source from the list to identify the target user population for this policy.

**Available Identity Sources**

Identity Source	Available to Policy
On-Prem AD	<input checked="" type="checkbox"/>

Cancel Next Step

Status: Success ✓ Publish Changes

Home Users ▾ Access ▾ Applications ▾ Authentication Clients ▾ Platform ▾ Dashboards ▾ Help My Account ▾ Sign Out

#### MFA Policy

**Basic Information**

Enable primary authentication if RSA will manage all authentication to resources protected by this policy (2.0 policy). If you do not enable primary authentication, then this policy can only be used for additional authentication (1.0 policy).

**Identity Sources**

**Primary Authentication**

This policy is in use and you cannot toggle primary authentication. If you want to turn primary authentication on or off please unassign this policy from any clients.

**Rule Sets**

Enable Disable

Select the methods you want to make available for primary authentication.

**Default Method**

Password

**Alternate Methods**

Authenticate OTP

ADD

Cancel Next Step

MFA Policy

Rule Set Name: Allow All Authenticated Users

Target Population: Apply to All Users

Access Details: Access Allowed, Conditional

Additional Authentication: Required

Assurance Level: Low

Authentication Options: Approve, Authenticate OTP, FIDO, QR Code, Includes Medium and High Options

-RSA Authentication API Key  
 -RSA Authentication API REST URL

Company Settings

Company Information: The Authentication API requires unique keys for communication between a client and the Cloud Authentication Service. Use secure methods to provide these keys to your web development team. You can add up to 10 keys.

Customization Settings: SecurID Authentication API REST URL: https://la4.auth-demo.securid.com:443 / Copy URL

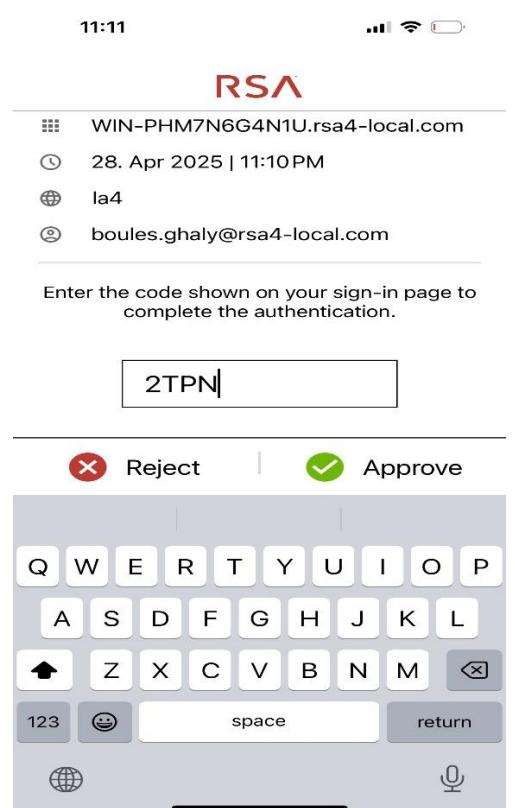
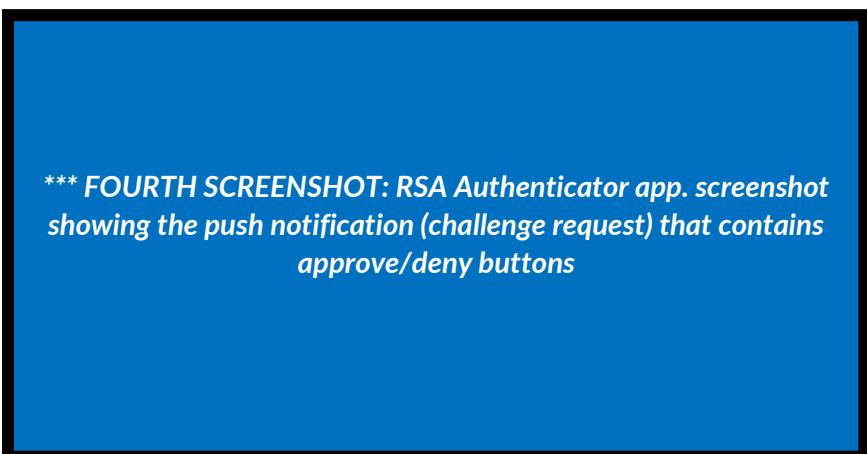
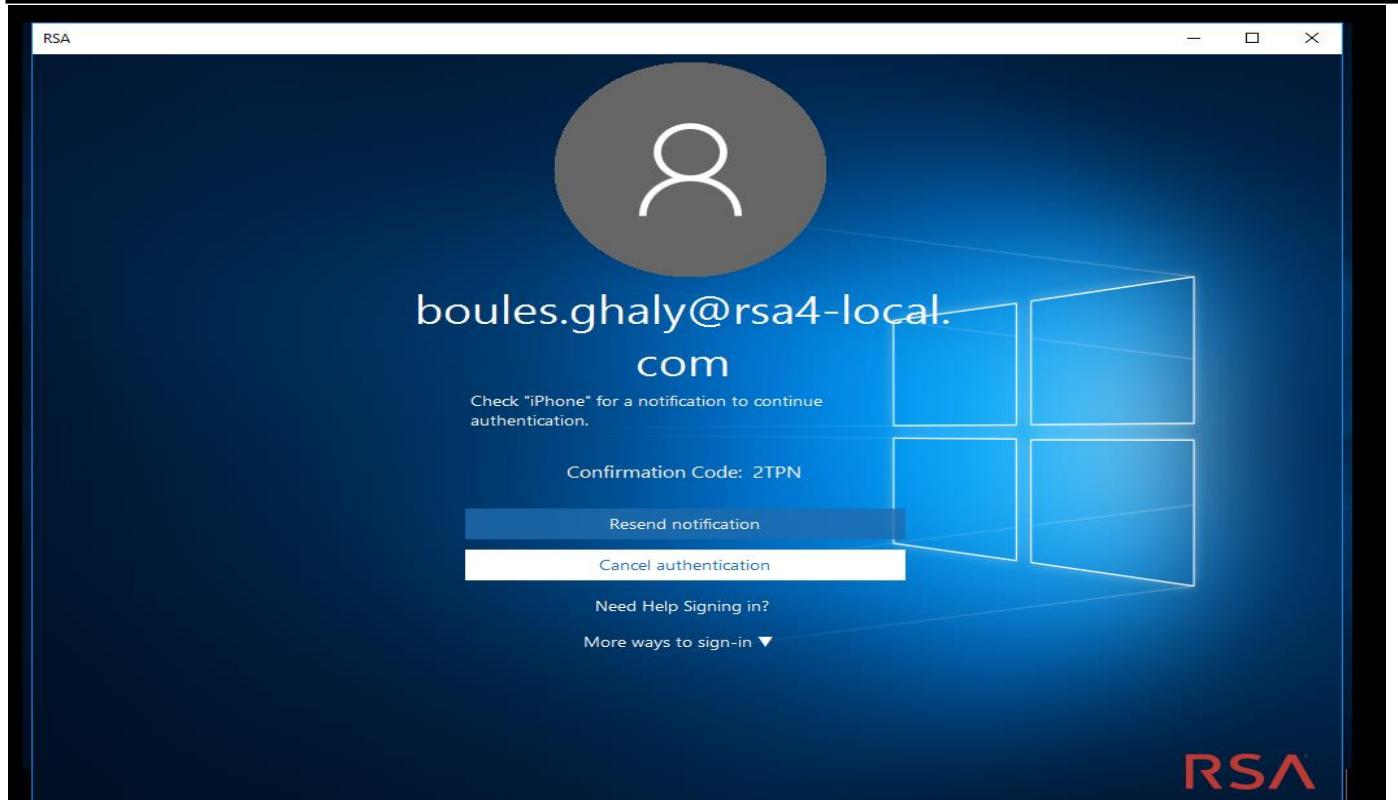
Sessions & Authentication: Authentication API Keys

Email Notifications: View existing keys and add new ones.

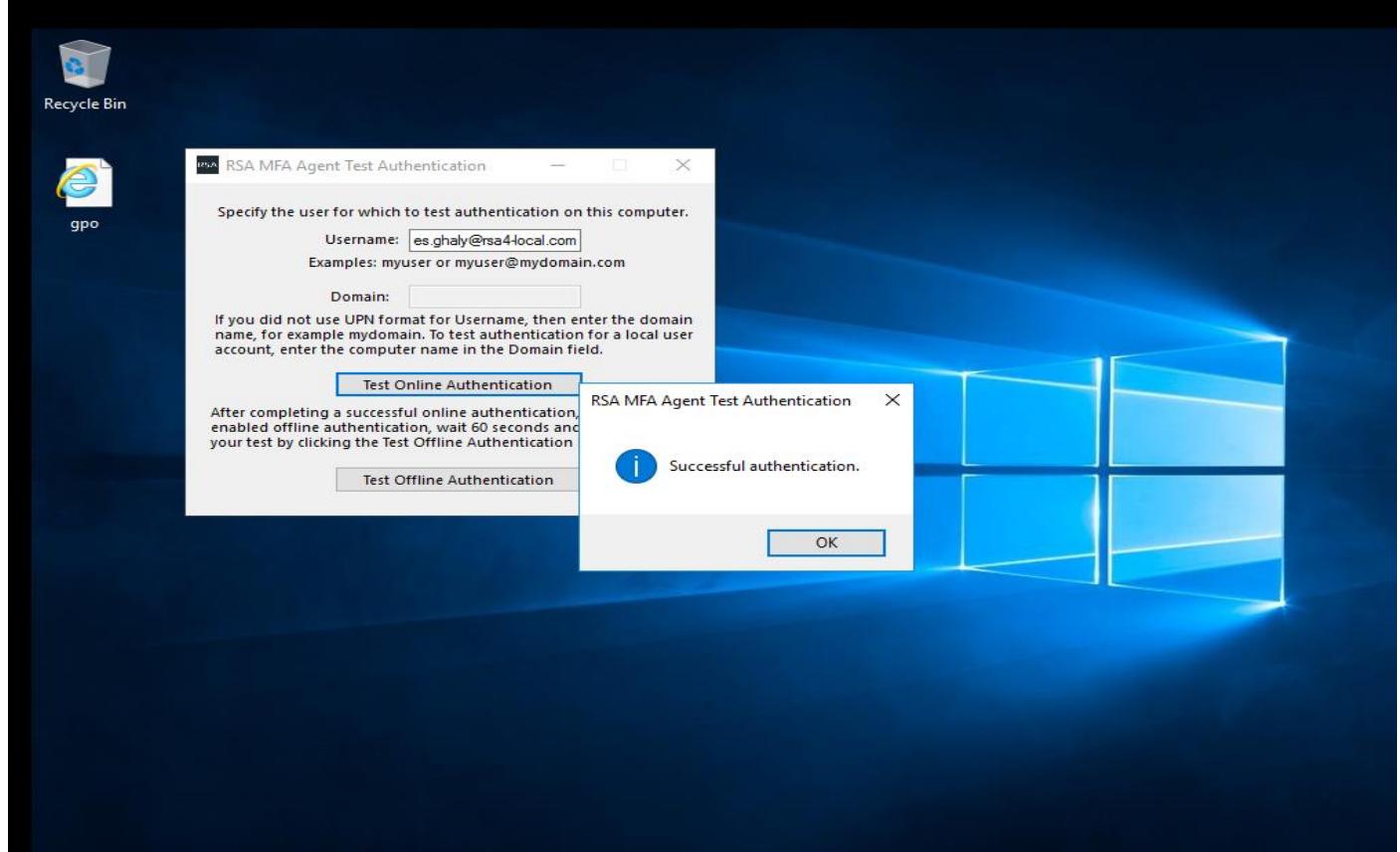
Description	Network Zone (Optional)
Description	None
Key: 75835c038a7a8ed775c16712504bc55ec4be77c0	
<a href="#">+ ADD</a>	

### 3. RSA MFA Agent Authentication

**\*\*\* THIRD SCREENSHOT:** The RSA MFA Agent additional authentication page showing the push notification and code matching feature as a result of testing ONLINE Authentication



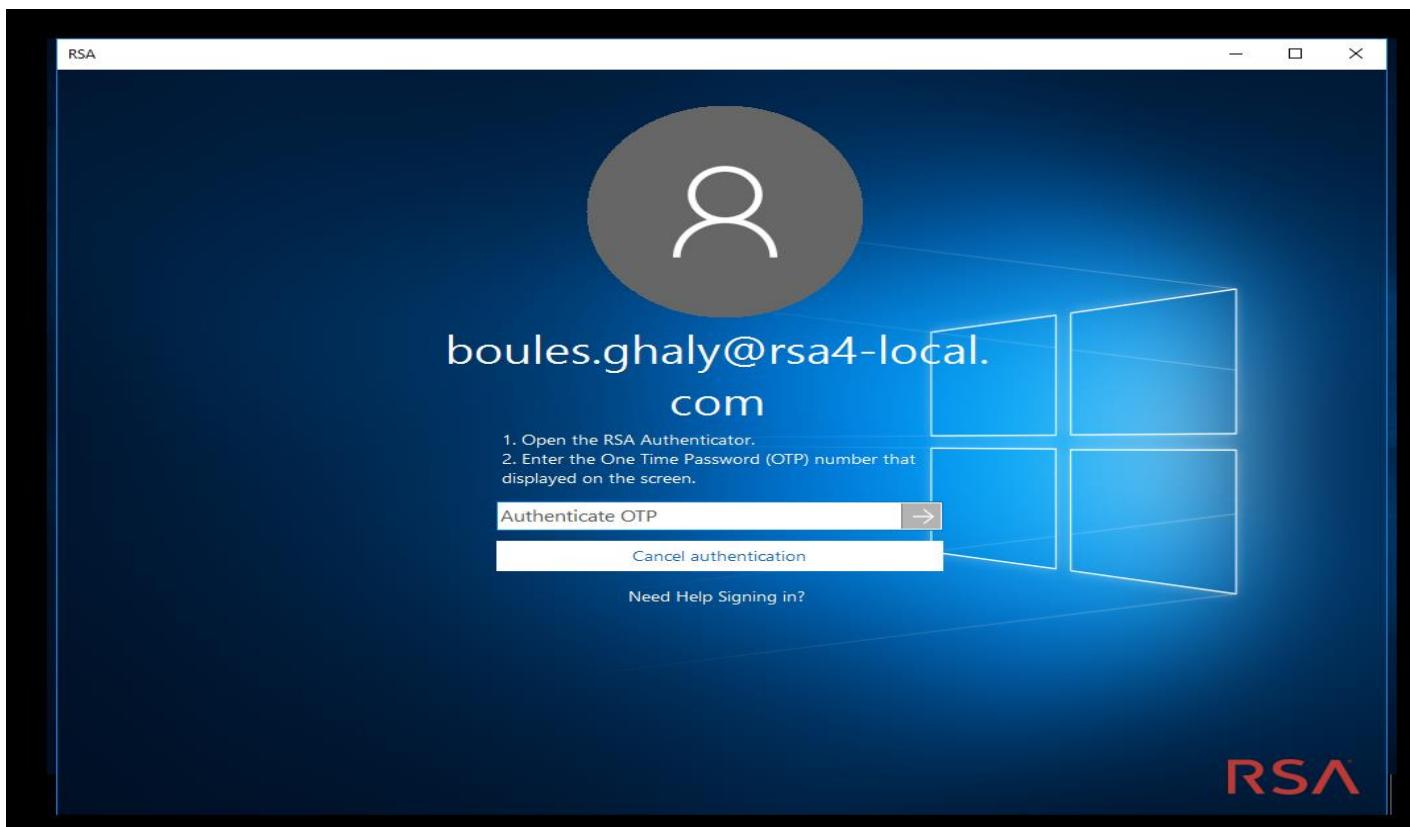
**\*\*\*FIFTH SCREENSHOT: RSA MFA Agent Test Authentication Result (Successful/Failed authentication)**



**\*\*\*SIXTH SCREENSHOT: User authentication activity from the RSA CAS User Event Monitor showing successful authentication against RSA MFA Agent**

Transaction ID	Timestamp	User ID	Event Code	Description	Application	Assurance Level	Method	Authentication Details
348e7185-02ba-4cdb-90a7-7136618ab1fd	Apr 28, 2025 01:11 PM PDT	boules.ghaly@rsa4-local.com	3014	Offline day data download successful.	WIN-PHM7N6G4N1U.rsa4-local.com	BIOMETRICS		User ID:boules.ghaly@rsa4-local.com, userUuid:989d66d2-d8c7-99b3-7ac8-daeed12af0dc, Credential ID:620148555005, Name:iPhone

**\*\*\*SEVENTH SCREENSHOT: The RSA MFA Agent additional authentication page showing the push notification and code matching feature as a result of testing OFFLINE Authentication**



#### 4. RADIUS client Configurations

**\*\*\*EIGHTH SCREENSHOT: RADIUS Client configurations on the RSA CAS side**

A screenshot of a web-based configuration interface for a RADIUS client. The top navigation bar includes links for Home, Users, Access, Applications, Authentication Clients, Platform, Dashboards, Help, My Account, and Sign Out. The main title is "Edit RADIUS Client". On the left, there is a sidebar with tabs for "RADIUS Client" (which is selected) and "RADIUS Profiles". The main form fields include: "Name" (Project Raduis client), "Description (optional)" (for project), "IP Address" (192.168.95.130), "Shared Secret" (a masked password), and "Authentication Details" (radio buttons for Cloud Authentication Service validation). At the bottom, there is a status message about status updates and a copyright notice for RSA Security LLC.

## Edit RADIUS Client

[?](#)

Cancel

Save and Next Step

## RADIUS Client

## RADIUS Profiles

Name

Project Raduis client

Description (optional)

for project

IP Address

192.168.95.130

Shared Secret ⓘ

\*\*\*\*\*

## Authentication Details

- Cloud Authentication Service validates password and applies access policy for additional authentication.
- Cloud Authentication Service only applies access policy for additional authentication.

 For status updates, subscribe to [status.securid.com](http://status.securid.com).

© 2015-2025 RSA Security LLC or its affiliates. All rights reserved.
**NOTE: RADIUS does not support TOTP, QR code or method combinations such as**

## 1.0 Access Policy ⓘ

## MFA Policy



## ▼ Advanced Configuration

## Company Settings

[?](#)

Cancel

Save Settings

## Company Information

## Customization Settings

## Sessions &amp; Authentication

## Authentication API Keys

## Email Notifications

Configure the code matching method presented to the user as part of the push notification.

Select the confirmation code method available to the user:

- Input
- Selection
- Visual Confirmation
- None

Strict code matching enforcement ⓘ

 Disabled

Length

4

- Allow numbers
- Allow alpha characters

5.

RADIUS

client

Authentication

\*\*\*NINTH SCREENSHOT: RADIUS Client configurations on the RSA CAS side

ALREADY done Above in part 4

DefaultApplianceCluster\_Learn Access 4

Cancel

Save and Finish

Configure basic details and high availability settings for the cluster.

Cluster Name

DefaultApplianceCluster\_Learn Access 4

These settings do not apply to the identity router that is embedded in Authentication Manager.

- Enable the SSO service on all identity routers in the cluster. i
- Enable the RADIUS service on all identity routers in the cluster.

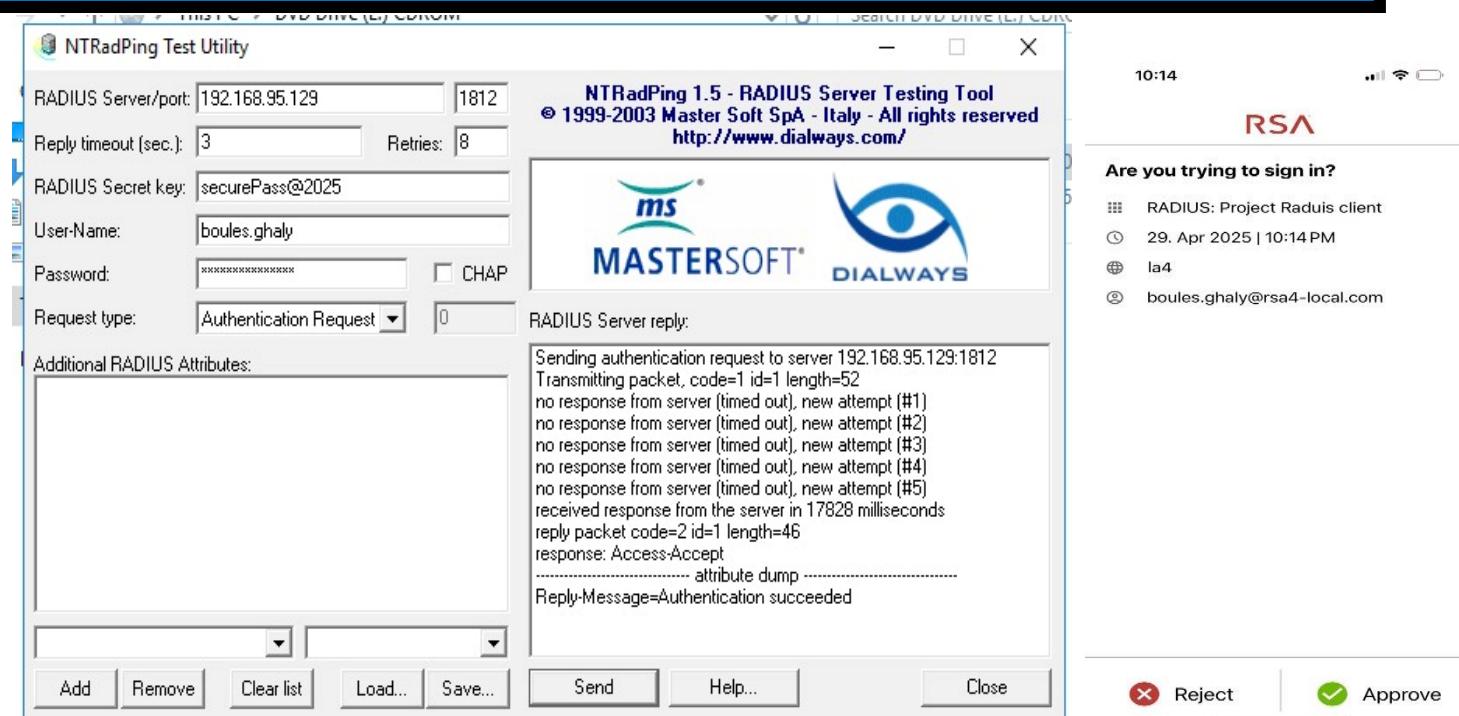
#### High Availability

Enabled Disabled

Cancel

Save and Finish

\*\*\* TENTH SCREENSHOT: RSA Authenticator app. screenshot showing the push notification (challenge request) that contains approve/deny buttons



**\*\*\*ELEVENTH SCREENSHOT: User authentication activity from the RSA CAS User Event Monitor showing successful authentication against RADIUS client**

Showing 1 - 10 of 10 Results

Filter:	User ID/Transaction ID	Last:	4 hours	All Events	Search	<input type="checkbox"/> Include Verbose Logs		
Transaction ID	Timestamp	User ID	Event Code	Description	Application	Assurance Level	Method	Authentication Details
9dd7945e-7d70-4812-8fb0-d0c6ea709a90	Apr 29, 2025 12:14 PM PDT	boules.ghaly@rsa4-local.com	20302	Multifactor authentication succeeded.	RADIUS: Project Raduis client			Policy Name: MFA Policy; attempt_id: bf10e279...
9dd7945e-7d70-4812-8fb0-d0c6ea709a90	Apr 29, 2025 12:14 PM PDT	boules.ghaly@rsa4-local.com	801	Biometric authentication succeeded.	RADIUS: Project Raduis client	Low	BIOMETRICS	attempt_id: bf10e279...

# RSA