



(NETW 1002)

Systems and Network Security Milestone 2 Submission Report

OWN YOUR
IDENTITY.

Milestone 2 Report Submission:

Virtual Machines Network Settings:

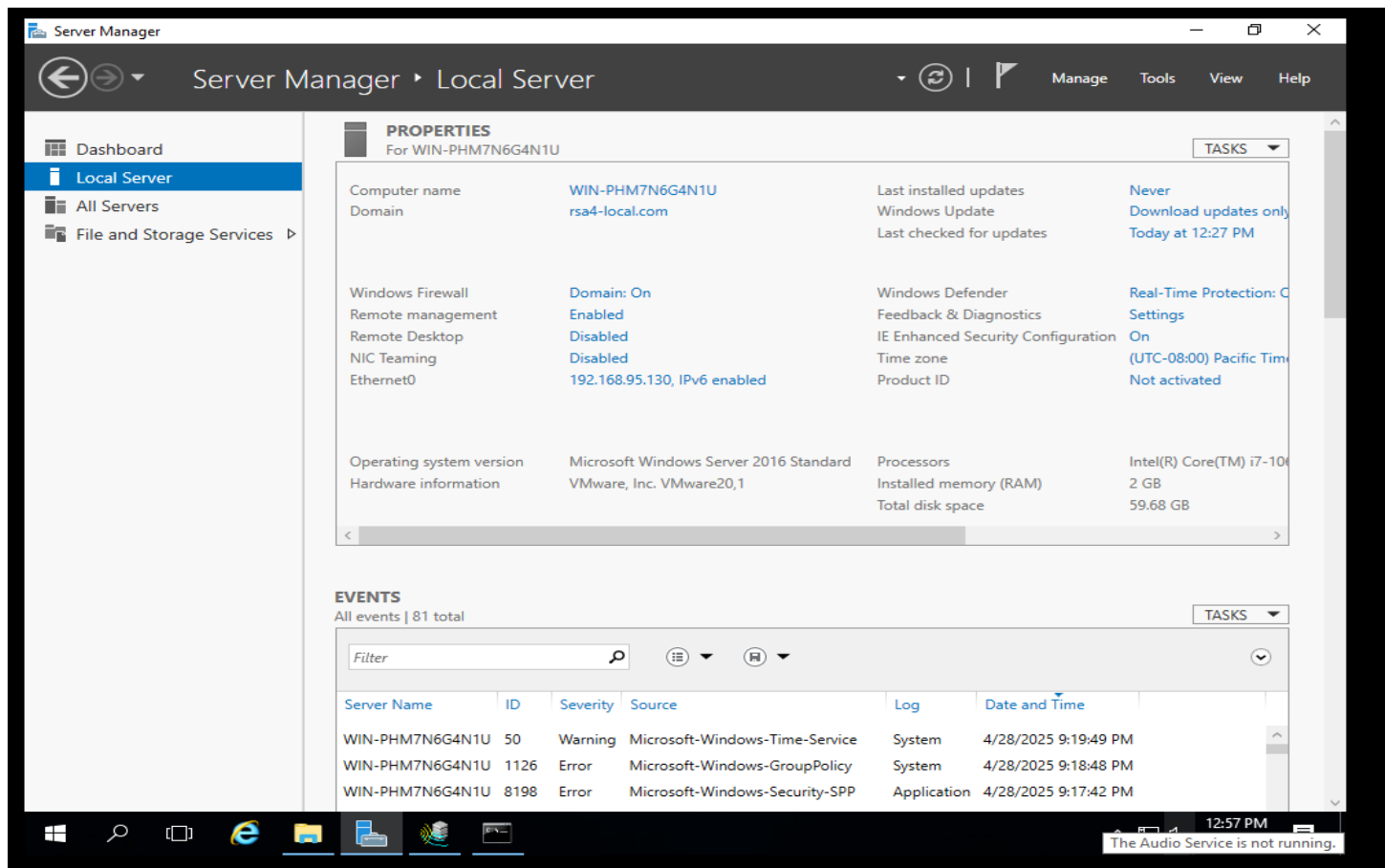
- Virtual Machine #3:

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

- ✓ No Errors Detected
- ⚠ A fast link was detected [More information...](#)

No data available.

Computer Details

General

Computer name: RSA4-LOCAL\WIN-PHM7N6G4N1U
Domain: rsa4-local.com
Site: Default-First-Site-Name
Security Group Membership: [show](#)

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	View Log
Registry	Success	94 Millisecond(s)	4/28/2025 12:03:52 PM	View Log
Security	Success	297 Millisecond(s)	4/25/2025 10:37:43 AM	View Log

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

Select the users to challenge

Challenge: Users In a group

Enter the name of the challenge group in the format <domain name or machine name>\<group name>.

For example: CORP\SecurID Users

Group name: rsa4-local\Project

Secondary Group name:

Policy	Setting	Winning GPO
Specify logging options	Enabled	Local Group Policy

Select the log level.

Verbose

Select the number of log files to rotate.

5

Select the log file size.

MB:

5

Enter the path to store log files.

Select the components to include in the log files.

OfflineAuthentication

Enabled

RsaMfaAgentTestAuthentication

Enabled

SIDAccessCredentialProvider

Enabled

SIDAccessNotificationIcon

Enabled

SIDAccessPasswordLessCredentialProvider

Enabled

Policy	Setting	Winning GPO
Specify the user name format sent to the RSA authentication server	Enabled	Local Group Policy

Specify the User Name Format.

Format:

UPN

Specify Excluded Domains (optional)

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



RSA4-LOCAL\WIN-PHM7N...



SIDAccessPasswordLessCredentialProvider

Enabled

Policy	Setting	Winning GPO
Specify the user name format sent to the RSA authentication server	Enabled	Local Group Policy

Specify the User Name Format.

Format:

UPN

Specify Excluded Domains (optional)

Domains:

RSA recommends listing both the DNS and Windows NTLM domain name.

For example, to exclude a domain with a DNS name of 'corp.domain.com' and a Windows NTLM name of 'CORP', enter the following:

CORP,corp.domain.com

RSA Desktop/RSA Settings

Policy	Setting	Winning GPO
Cloud Authentication Service Access Policy	Enabled	Local Group Policy

Enter the exact name of the access policy as specified in the Cloud Administration Console.

MFA Policy

Policy	Setting	Winning GPO
Enable RSA authentication	Enabled	Local Group Policy
RSA Authentication API Key	Enabled	Local Group Policy

Enter the RSA Authentication API Key.

75835c038a7a8ed775c16712504bc55ec4be77c0

Policy	Setting	Winning GPO
RSA Authentication API REST URL	Enabled	Local Group Policy

Enter the RSA Authentication API REST URL.

https://la4.auth-demo.securid.com:443/

Policy Objects

Monday, April 28, 2025

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

[Cancel](#)[Next Step](#)

Basic Information

All fields are required (except where noted)

Name and Description

Name

Description (optional)

[Cancel](#)[Next Step](#)

Status: Success

Publish Changes

Home

Users

Access

Applications

Authentication Clients

Platform

Dashboards

Help

My Account

Sign Out

MFA Policy

[Cancel](#)[Next Step](#)

Basic Information

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

[Cancel](#)[Next Step](#)

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).

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.

[Enable](#) [Disable](#)

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

Default Method

Password

Alternate Methods

Authenticate OTP

ADD

[Cancel](#)[Next Step](#)

Python cms.guc.edu.g... You are signed... (732) YouTube... 2025 WIDS Da... RSA RSA 1 - M2 descri... F1_macro Multi... You are signed... Google

https://la4.access-demo.securid.com/AdminInterface/customer/658/#policies/edit/9d61ba88-c3c5-ed3b-7195-3cd03f4a4ad

RSA Status: Success [Publish Changes](#)

Learn Access 4 Home Users **Access** Applications Authentication Clients Platform Dashboards Help My Account Sign Out

MFA Policy

[Basic Information](#)
[Identity Sources](#)
[Primary Authentication](#)
[Rule Sets](#)

[Cancel](#) [Save and Finish](#)

Rule Set Name
Allow All Authenticated Users

Target Population
Apply to [All Users](#) [Selected Users](#)

Access Details
Access [Allowed](#) [Conditional](#)

Additional Authentication [Required](#) [Not Required](#)

Assurance Level [Low](#)

Authentication Options [Approve](#)
[Authenticate OTP](#)
[FIDO](#)
[QR Code](#)
Includes Medium and High Options

For status updates, subscribe to [status.securid.com](#).
© 2015-2025 RSA Security LLC or its affiliates. All rights reserved.

- RSA Authentication API Key
- RSA Authentication API REST URL

Python cms.guc.edu.g... You are signed... (732) YouTube... 2025 WIDS Da... RSA RSA 1 - M2 descri... F1_macro Multi... You are signed... Google

https://la4.access-demo.securid.com/AdminInterface/customer/658/#company_settings/

RSA Status: Success [Publish Changes](#)

Learn Access 4 Home Users **Access** Applications Authentication Clients Platform Dashboards Help **My Account** Sign Out

Company Settings

[Company Information](#)
[Customization Settings](#)
[Sessions & Authentication](#)
[Authentication API Keys](#)
[Email Notifications](#)

[Cancel](#) [Save Settings](#)

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.

SecurID Authentication API REST URL [https://la4.auth-demo.securid.com:443/](#) [Copy URL](#)

Authentication API Keys

View existing keys and add new ones.

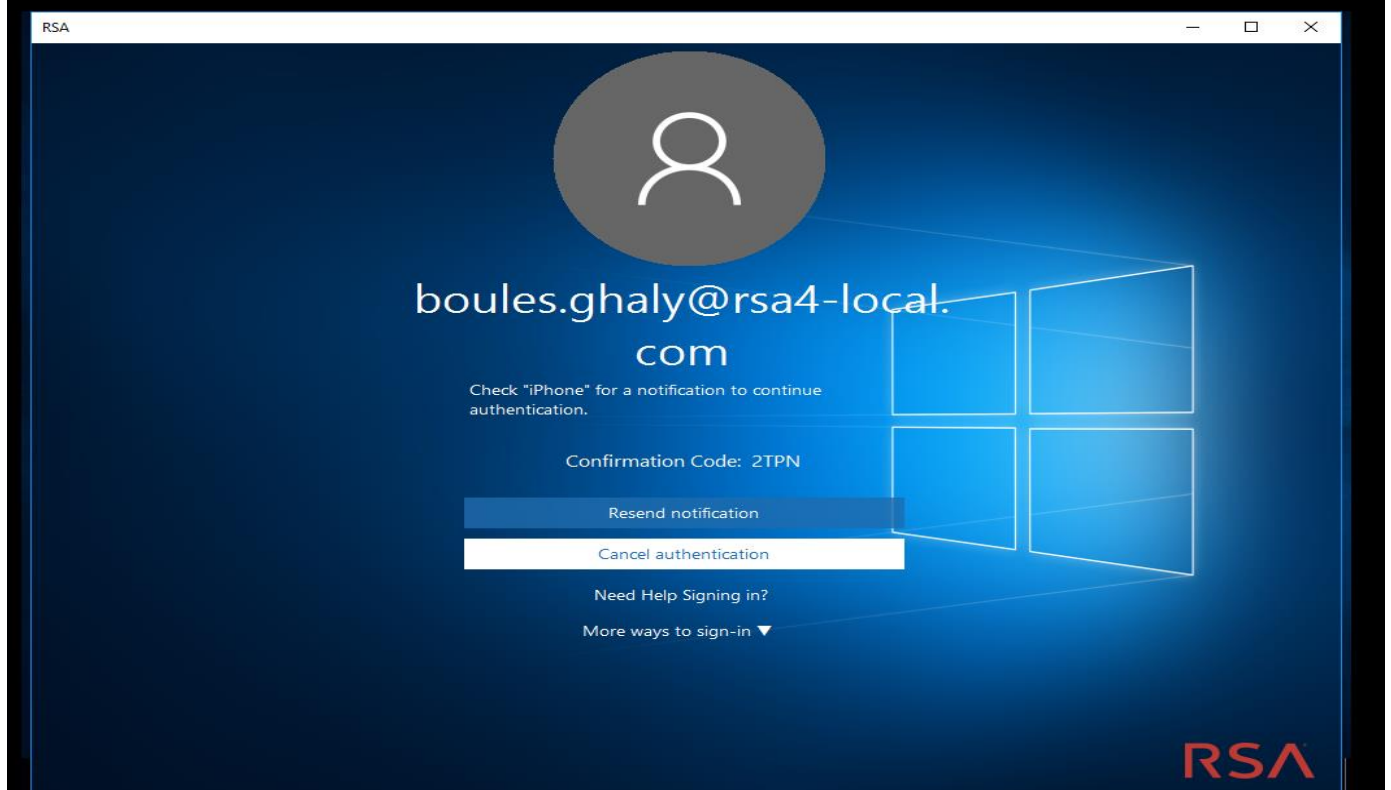
Description	Network Zone (Optional)
<input type="text" value="Description"/>	<input type="text" value="None"/>
Key: 75835c038a7a8ed775c16712504bc55ec4be77c0	
+ ADD	

[Cancel](#) [Save Settings](#)

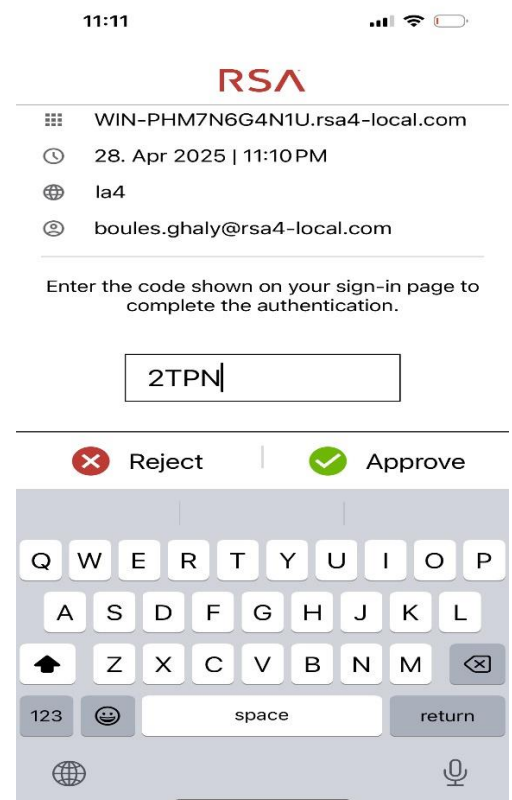
For status updates, subscribe to [status.securid.com](#).
© 2015-2025 RSA Security LLC or its affiliates. All rights reserved.

3. RSA MFA Agent Authentication

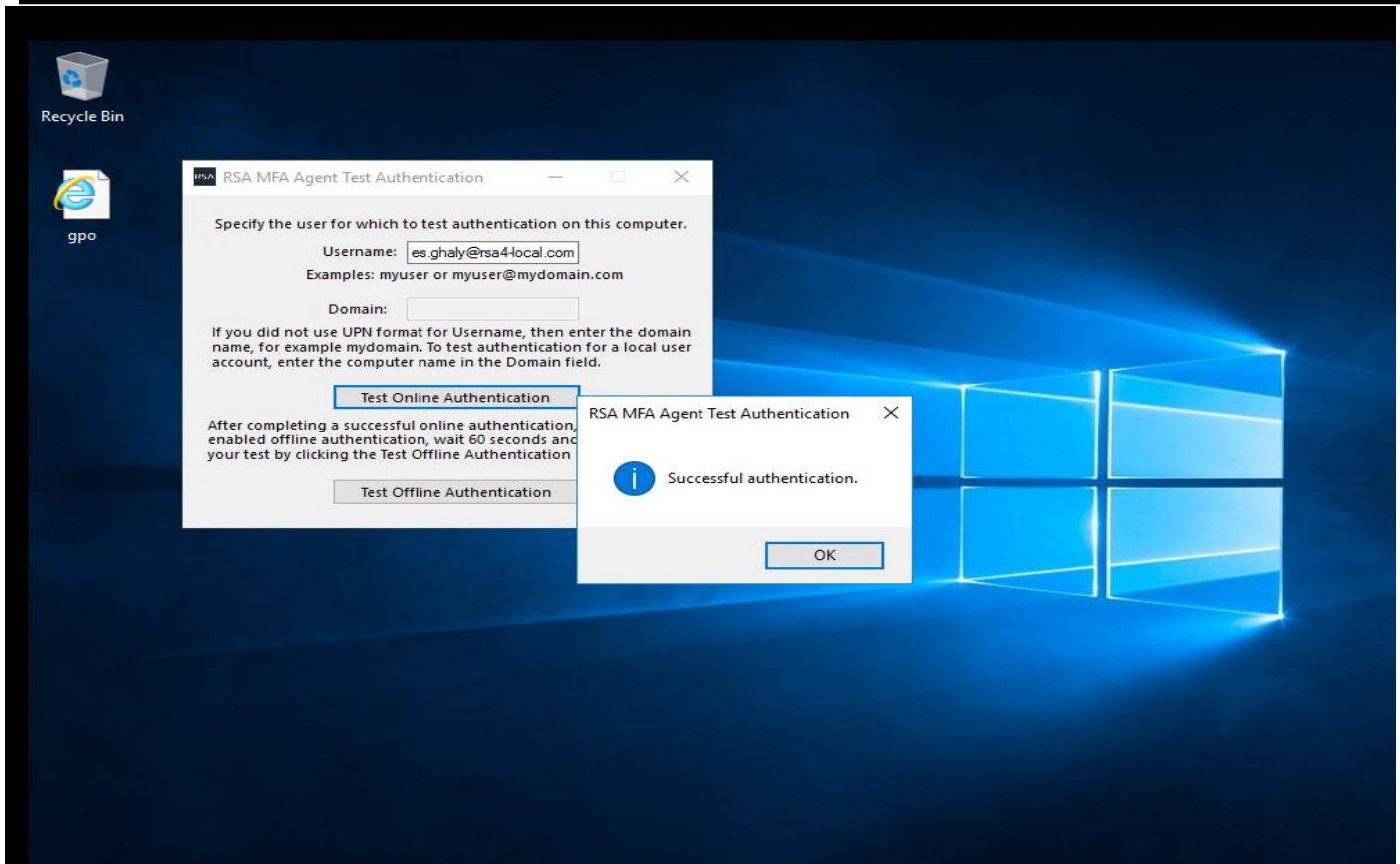
***** THIRD SCREENSHOT: The RSA MFA Agent additional authentication page showing the push notification and code matching feature as a result of testing ONLINE Authentication**



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



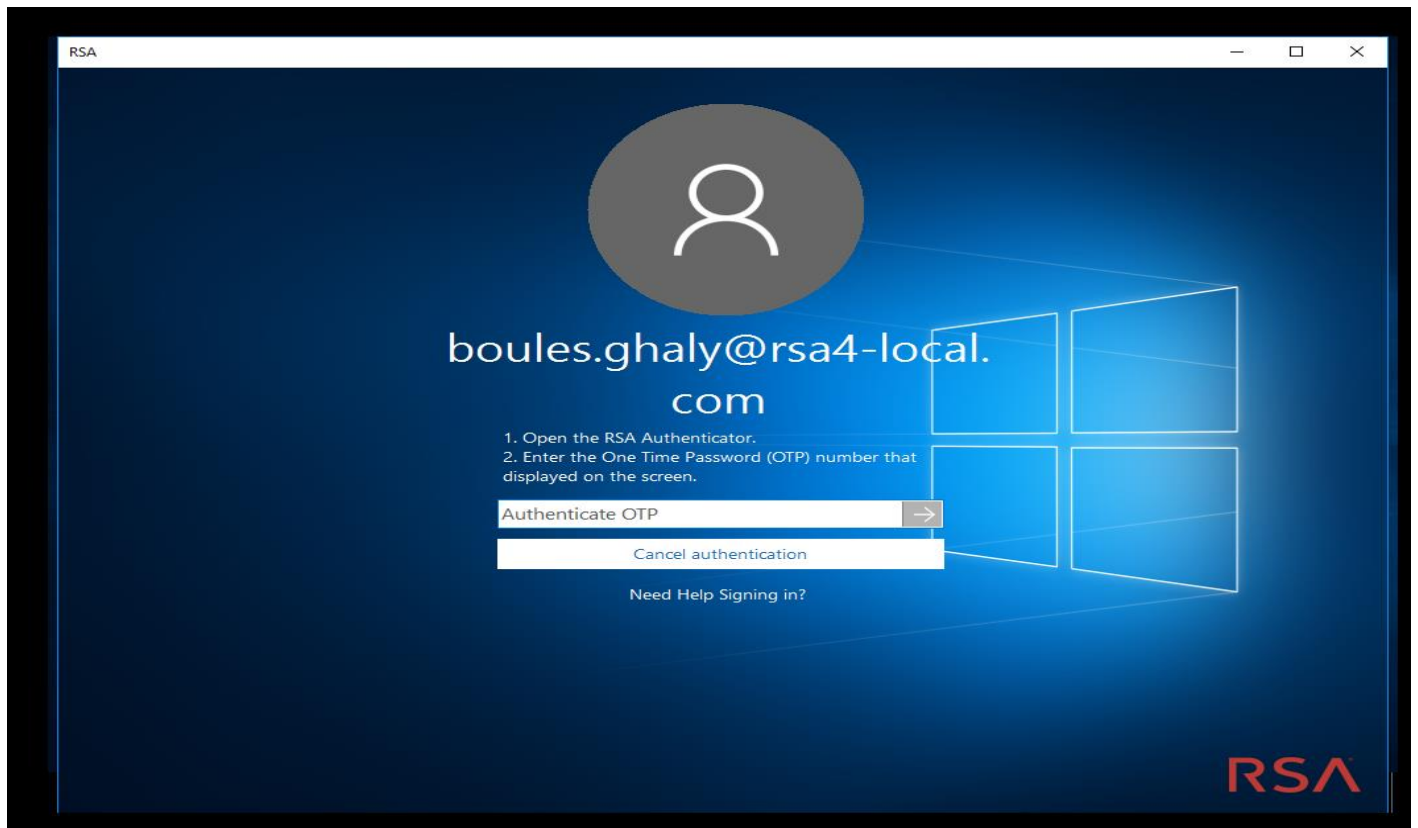
*****FIFTH SCREENSHOT: RSA MFA Agent Test Authentication Result (Successful/Failed authentication)**



*****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,userUID: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**

Learn Access 4 Home Users v Access v Applications v Authentication Clients v Platform v Dashboards v Help My Account v Sign Out

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.

© 2015-2025 RSA Security LLC or its affiliates. All rights reserved.

Edit RADIUS Client



Cancel

Save and Next Step

RADIUS Client

RADIUS Profiles

Name

Project Radius 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.

© 2015-2025 RSA Security LLC or its affiliates. All rights reserved.

NOTE: RADIUS does not support FIDO, QR Code or method combinations such as

1.0 Access Policy

MFA Policy



Advanced Configuration

RSA

Status: Success

Publish Changes

Learn Access 4

Home

Users

Access

Applications

Authentication Clients

Platform

Dashboards

Help

My Account

Sign Out

Company Settings



Cancel

Save Settings

Company Information

Customization Settings

Sessions & 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

***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.

☒ 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

NTRadPing Test Utility

RADIUS Server/port: 192.168.95.129 1812

Reply timeout (sec.): 3 Retries: 8

RADIUS Secret key: securePass@2025

User-Name: boules.ghaly

Password: ☐ CHAP

Request type: Authentication Request

Additional RADIUS Attributes:

NTRadPing 1.5 - RADIUS Server Testing Tool
 © 1999-2003 Master Soft SpA - Italy - All rights reserved
<http://www.dialways.com/>

MASTERSOFT® **DIALWAYS**

RADIUS Server reply:

```

Sending authentication request to server 192.168.95.129:1812
Transmitting packet, code=1 id=1 length=52
no response from server (timed out), new attempt (#1)
no response from server (timed out), new attempt (#2)
no response from server (timed out), new attempt (#3)
no response from server (timed out), new attempt (#4)
no response from server (timed out), new attempt (#5)
received response from the server in 17828 milliseconds
reply packet code=2 id=1 length=46
response: Access-Accept
..... attribute dump .....
Reply-Message=Authentication succeeded
  
```

Add Remove Clear list Load... Save... Send Help... Close

10:14

RSA

Are you trying to sign in?

RADIUS: Project Raduis client

29. Apr 2025 | 10:14 PM

la4

boules.ghaly@rsa4-local.com

☒ Reject

☒ Approve

***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:	<input type="text" value="User ID/Transaction ID"/>	Last:	<input type="text" value="4"/>	<input type="text" value="hours"/>	<input type="text" value="All Events"/>	<input type="button" value="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