RSA SecurID Access Implementation Guide

XYPRO Technology Corporation

XYGATE User Authentication 2.25

Certified: August 23, 2019

Table of Contents

Solution Summary

This section describes the ways in which XYPRO XYGATE UA can integrate with RSA SecurID Access. Use this information to determine which integration type your deployment will employ.

Use Case

User Sign-In - When integrated, users must authenticate with RSA SecurID Access in order to sign into the HPE NonStop using XYGATE User Authentication (XUA). User Sign-In can be integrated with RSA SecurID Access using **SecurID Authentication API** and **Authentication Agent**.

Integration Types

SecurID Authentication API integrations can provide a rich user interface with all RSA SecurID Access features within the partner application. Refer to the Supported Features section in this guide see which features this partner application has implemented.

Authentication Agent integrations use an embedded RSA agent to provide RSA SecurID and Authenticate Tokencode authentication methods within the partner's application. Authentication agents are simple to configure and support the highest rate of authentications.

Supported Features

This section shows all of the supported features by integration type and by RSA SecurID Access component. Use this information to determine which integration type and which RSA SecurID Access component your deployment will use. The next section contains the steps to integrate RSA SecurID Access with XYPRO XYGATE UA for each integration type.

XYPRO XYGATE UA Integration with RSA Cloud Authentication Service

Authentication Methods	Authentication API	RADIUS	Relying Party	SSO Agent
RSA SecurID	✔	-	-	-
LDAP Password	✔	-	-	-
Authenticate Approve	✔	-	-	-
Authenticate Tokencode	✔	-	-	-
Device Biometrics	✔	-	-	-
SMS Tokencode	-	-	-	-
Voice Tokencode	-	-	-	-
FIDO Token	n/a	n/a	-	-

XYPRO XYGATE UA Integration with RSA Authentication Manager

Authentication Methods	Authentication API	RADIUS	Authentication Agent
RSA SecurID	✔	-	✔
On-Demand Authentication	✔	-	✔
Risk-Based Authentication	n/a	-	-

✔ Supported

- Not supported

n/t Not yet tested or documented, but may be possible.

Configuration Summary

The following links provide instructions on how to integrate XYPRO XYGATE UA with RSA SecurID Access.

This document is not intended to suggest optimum installations or configurations. It assumes the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components. All RSA SecurID Access and XYPRO XYGATE UA components must be installed and working prior to the integration.

Integration Configuration

- Authentication Agent
- SecurID Authentication API with AM
- SecurID Authentication API with CAS

Certification Details

Date of testing: May 14, 2019

RSA Cloud Authentication Service

RSA Authentication Manager 8.4, Virtual Appliance

XYPRO XYGATE UA 2.25

Known Issues

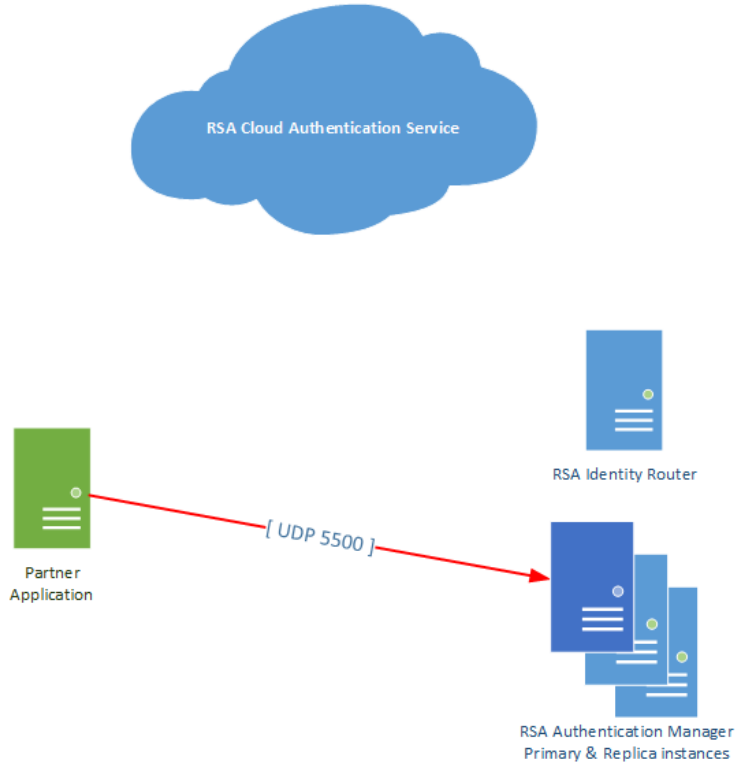
No known issues.

Integration Configuration

Authentication Agent

This section describes how to integrate RSA SecurID Access with XYPRO XYGATE UA as an authentication agent.

Architecture Diagram



Configure RSA Authentication Manager

To configure your RSA Authentication Manager for use with an authentication agent, you must create an agent host record in the Security Console of your Authentication Manager and download its configuration file (sdconf.rec).

Agent host record configuration differs slightly depending on whether you are using a UDP-based agent (using 8.1.x or earlier RSA Agent API) or TCP-based agent (using 8.5 or newer RSA Agent API).

If UDP-based agent:

- Hostname: Configure the agent host record name to match the hostname of the agent.
- IP Address: Configure the agent host record to match the IP address of the agent.

Note: Authentication Manager must be able to resolve the IP address from the hostname

If TCP-based agent:

- Hostname: Configure the agent host record name to match the agent name as specified in the agent's configuration. It does not have to match the hostname of the authentication agent.
- IP Address: Leave blank. Any input to this field will be disregarded.

Configure XYPRO XYGATE UA

Perform these steps to configure XYPRO XYGATE UA as an authentication API client to RSA Authentication Manager.

Procedure

1. Download the sdconf.rec file from RSA Authentication Manager Security Console and copy to the **/rsa** directory in XUA.

2. Sign into NonStop as the XUA admin, and run XUA_RSA_INSTALL macro to configure the RSA interface. You will be asked a series of questions about configuring XUA to interface with the RSA service.

```
> RUN XUA
> XUA_RSA_INSTALL
```

Note: Responses to the RSA install macro will be recorded into the UACONF file as keywords using the values you enter at the prompts. These values can be modified in the UACONF only after the macro run is completed.

```
Do you want to configure the RSA interface <Y>?
```

3. Enter **Y** to configure the service.

```
What is the TCP/IP process name <$ZTCP2>?
```

4. Enter your **TCP/IP process name**.

```
How many seconds should XUA wait for a RSA response before timeout occurs<30>?
```

5. Enter **30**.

```
Do you want to use RSA authentication for all NonStop users <No>?
```

6. Answer according to your need.

```
Do you want to require a password in addition to the SecurID token for all NonStop
users <NO>?
```

7. Answer according to your need.

```
Is your RSA server configured as a web service <N>?
```

8. Enter **N**.

```
Do you want to configure the RSA interface now <Y>?
```

9. Enter **Y**.

Configuration is complete.

Note: Authenticating with the RSA SecurID Access requires the UAACL rule, UAGROUP, which maps NonStop user accounts to RSA user accounts and invokes RSA processing by XUA. Refer to XYGATE User Authentication Reference Manual for more information.

SecurID Agent Integration Details

RSA Authentication Agent API	5.1
RSA SecurID User Specification	All Users
Display RSA Server Info	No
Perform Test Authentication	Yes
Agent Tracing	Yes

RSA Authentication Agent Files (C and Java Agents)

Agent Files	Location
sdconf.rec	/rsa
sdopts.rec	/rsa
Node secret	/rsa
sdstatus.12 / jastatus.12	/rsa

Agent Tracing:

Enter the following from NonStop terminal as an administrator or as the installation owner:

```
> XUA_EXECUTE_RSA_PROXY TRACE
```

User Experience

User-defined new PIN:

```
TACL 1> logon sini_n_xypro
Enter PASSCODE:  XYGATEAC 5.80 XYPRO Support \X       20991231 (see <
 Copyright)

To continue you must enter a new PIN.
Are you ready to enter a new PIN? (y/n) [n]
Enter a new PIN between 4 and 8 alphanumeric
characters:
Re-enter new PIN to confirm:
PIN accepted. Wait for the tokencode to
change, then enter a new PASSCODE:

Welcome to the XYPRO Technology Corporation Computing Facility \X.

Last Logon:  11 AUG 2014, 10:34
Last Unsuccessful Attempt: 11 AUG 2014, 11:59  Total Failures: 31
TACL (T9205H01 - 01OCT2013), Operating System H06, Release H06.28.00
(C) Copyright 2005-2013 Hewlett Packard Development Company, L.P.
CPU 1, process has no backup
August 11, 2014 12:02:01
(Invoking $SYSTEM.SYSTEM.TACLLOCL)
(Invoking $VSNS.SINI.TACLCSTM)
**********************
Good Afternoon sini_n_xypro!
```

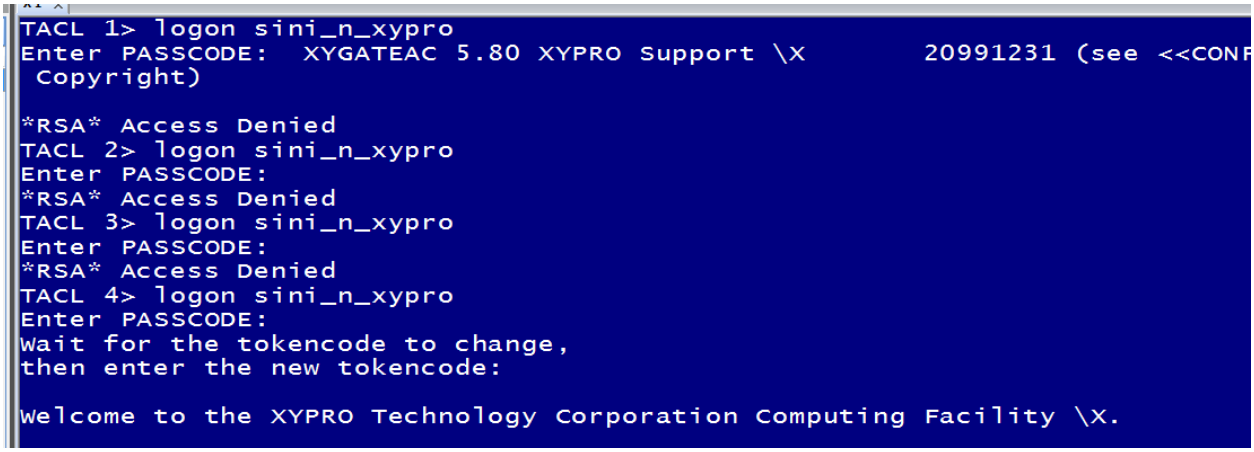
System-generated new PIN

```
TACL 1> logon sini_n_xypro
Enter PASSCODE:  XYGATEAC 5.80 XYPRO Support \X       20991231 (see <
 Copyright)

To continue, you must accept a new PIN generated
by the system  Are you ready to have the
system generate your PIN? (y/n) [n]


Your screen will automatically clear in 10 seconds.
Your new PIN is: iV6j
```

Next tokencode

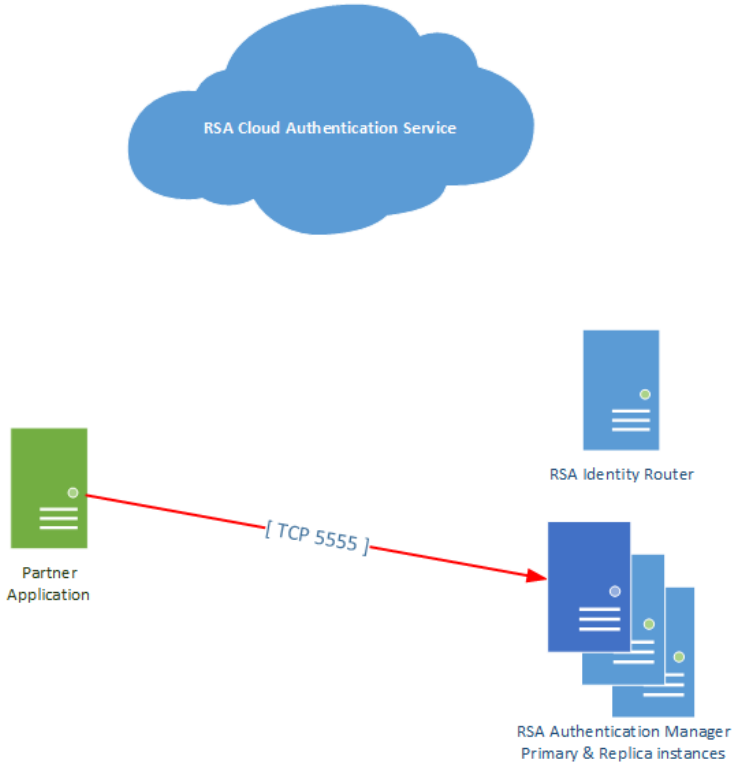


Return to the main page for more certification related information.

SecurID Authentication API with AM

This section describes how to integrate XYPRO XYGATE UA with RSA Authentication Manager using SecurID Authentication API.

Architecture Diagram



Configure RSA Authentication Manager

To configure the integration with RSA Authentication Manager, you must enable the REST Service and then create an authentication agent.

Sign into the **Security Console** and browse to **Setup** > **System Settings** > **REST Service**, mark the checkbox to enable **REST Service** and make note of the **Agent Credentials**. The Agent Credentials will be needed during configuration of the agent.

Browse to **Access** > **Authentication Agents** and click **Add New**. Enter the name of your authentication agent in the **Hostname** field and click **Save**.

Configure XYPRO XYGATE UA

Perform these steps to configure XYPRO XYGATE UA as an authentication API client to RSA Authentication Manager.

Procedure

1. Sign into NonStop as the XUA admin, and run XUA_RSA_INSTALL macro to configure the RSA interface. You will be asked a series of questions about configuring XUA to interface with the RSA service.

```
> RUN XUA
> XUA_RSA_INSTALL
```

Note: Responses to the RSA install macro will be recorded into the UACONF file as keywords using the values you enter at the prompts. These values can be modified in the UACONF only after the macro run is completed.

```
Do you want to configure the RSA interface <Y>?
```

2. Enter **Y** to configure the service.

```
What is the TCP/IP process name <$ZTCP2>?
```

3. Enter your TCP/IP process name.

```
How many seconds should XUA wait for a RSA response before timeout occurs<30>?
```

4. Enter **30**.

```
Do you want to use RSA authentication for all NonStop users <No>?
```

5. Answer according to your need.

```
Do you want to require a password in addition to the SecurID token for all NonStop
users <NO>?
```

6. Answer according to your need.

```
Is your RSA server configured as a web service <N>?
```

7. Enter Y.

```
RSA Hostname?
```

8. Enter the **hostname** or **IP address** of the RSA Authentication Manager you wish to authenticate with.

Example: rsarest.example.com

Note: An external high availability mechanism is required in order to use RSA Authentication Manager replica servers.

```
RSA access key?
```

9. Enter the **Access Key** from the RSA Authentication Manager Security Console.

```
Enter unqualified CACERT filename?
```

10. Enter the CACERT filename that will be used to validate the server certificate.

Example: RSACERT

```
RSA access ID?
```

Note: This value is not used by RSA SecurID Access. XYPRO recommends to specify the email address of the person who configures this integration.

```
RSA Language?
```

12. Enter the language code.

Example: en_US

```
RSA Port <5555>?
```

13. Enter the port that RSA Authentication Manager REST API is listening on. 5555 is the default value.

```
RSA Path?
```

14. Enter **/mfa/v1_1**

RSA Security key type <KEY>?

15. Enter **KEY**

```
RSA Agent name?
```

16. Enter the RSA agent name to match as configured in the RSA Authentication Manager security console.

```
RSA auth policy ID?
```

17. Leave blank. Any input will not be used.

```
RSA Attempt timeout (seconds)?
```

18. Enter 40.

```
Java install path </usr/tandem/nssjava/jdk180_h80>?
```

19. Enter the Java install path.

```
Do you want to configure the RSA interface now <Y>?
```

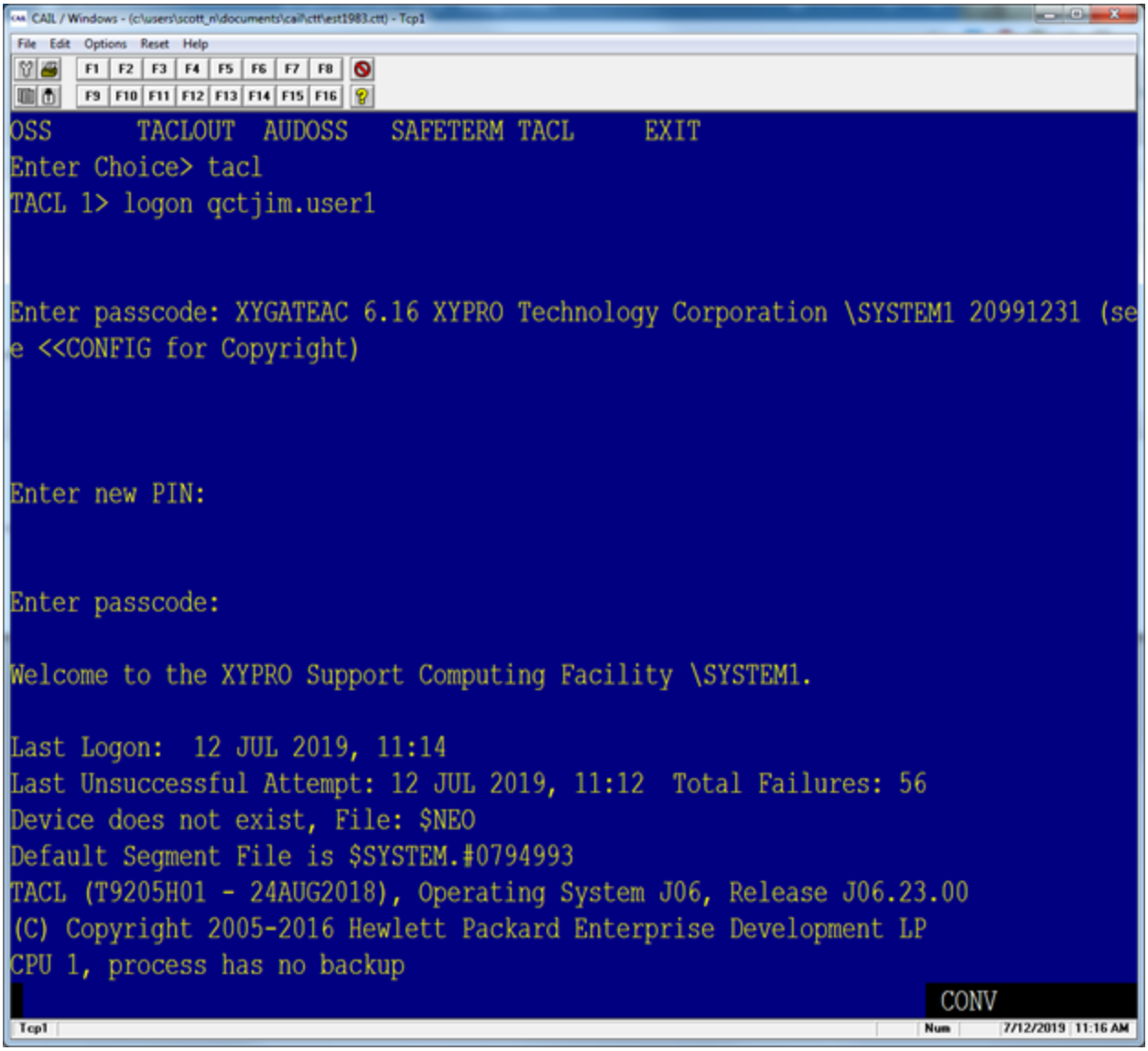
20. Enter **Y**.

Configuration is complete.

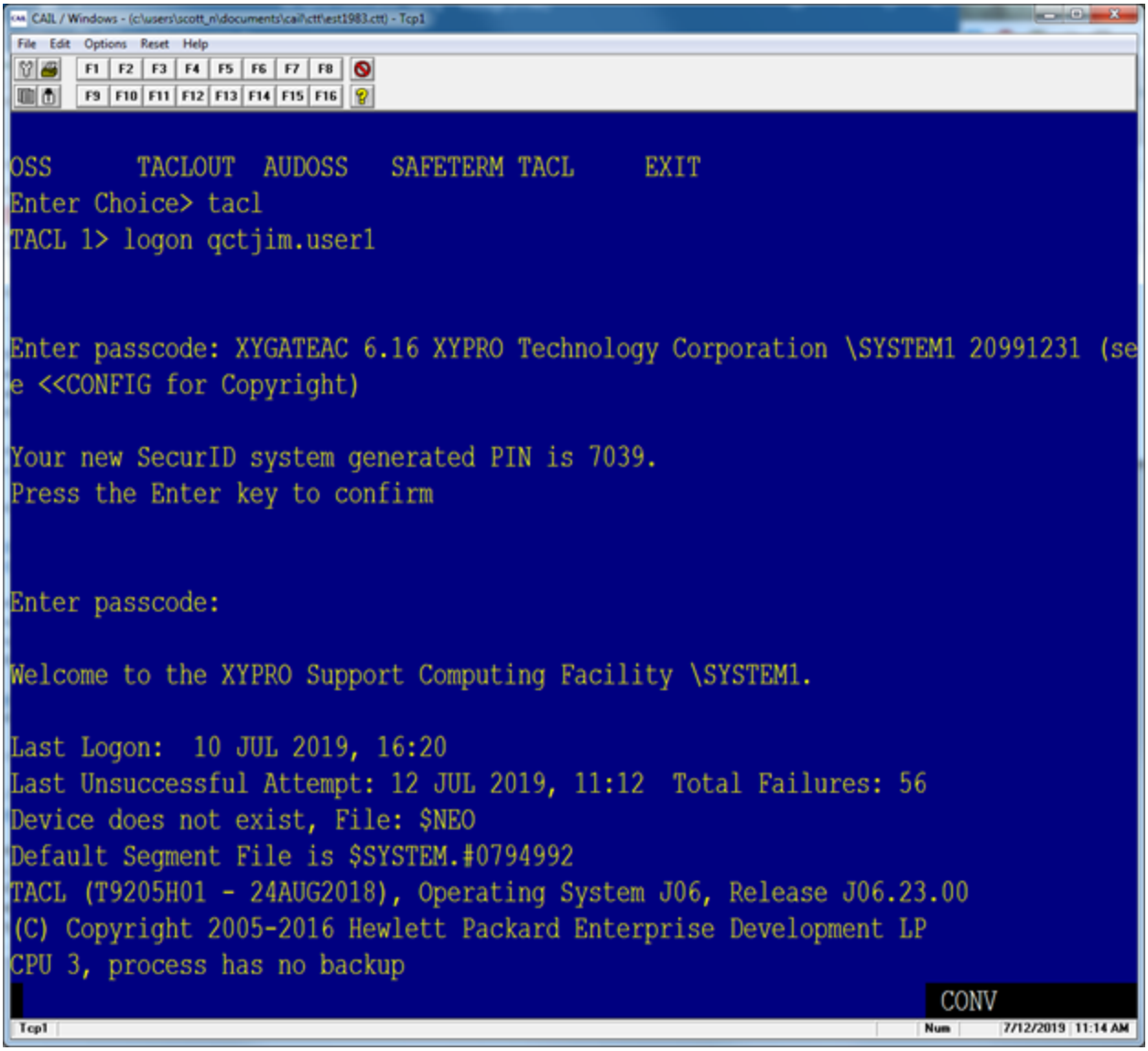
Note: Authenticating with the RSA SecurID Access requires the UAACL rule, UAGROUP, which maps NonStop user accounts to RSA user accounts and invokes RSA processing by XUA. Refer to XYGATE User Authentication Reference Manual for more information.

User Experience

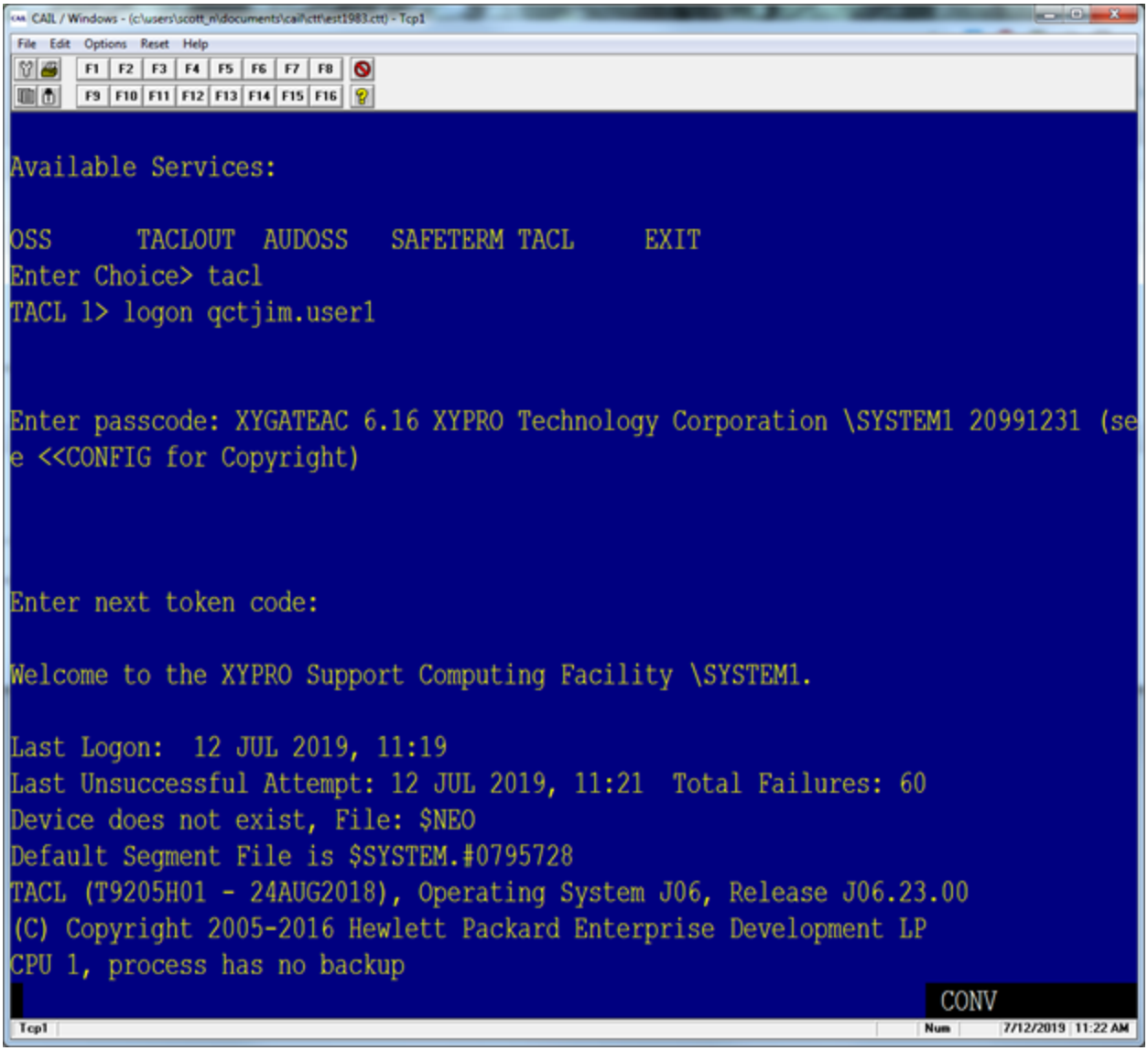
User defined new PIN



System-generated New PIN (AM):



Next Tokencode

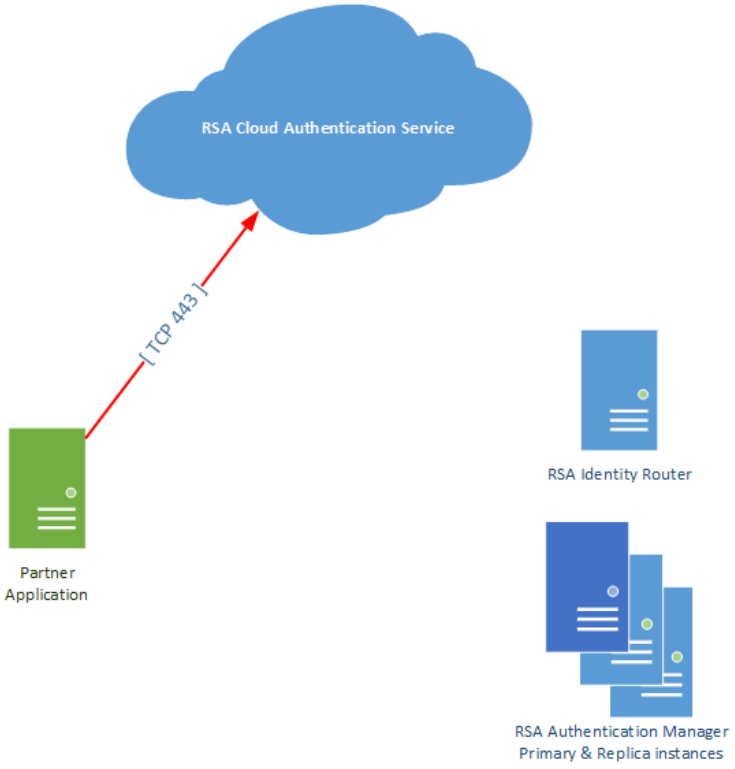


Return to the main page for more certification related information.

SecurID Authentication API with CAS

This section describes how to integrate XYPRO XYGATE UA with RSA Cloud Authentication Service using SecurID Authentication API.

Architecture Diagram



Configure RSA Cloud Authentication Service

To configure the integration with RSA Cloud Authentication Service, you must first collect the Authentication API key and Authentication Service Domain for your RSA SecurID Access tenant.

Sign into the Cloud Administration Console and browse to **My Account** > **Company Settings** > **Authentication API Keys** and copy the Description and Key.

Browse to **Platform** > **Identity Routers** > **Edit** > **Registration** and copy the **Authentication Service Domain**.

Configure XYPRO XYGATE UA

Perform these steps to configure XYPRO XYGATE UA as an authentication API client to RSA Cloud Authentication Service.

Procedure

1. Sign into NonStop as the XUA admin, and run XUA_RSA_INSTALL macro to configure the RSA interface. You will be asked a series of questions about configuring XUA to interface with the RSA service.

```
> RUN XUA
> XUA_RSA_INSTALL
```

Note: Responses to the RSA install macro will be recorded into the UACONF file as keywords using the values you enter at the prompts. These values can be modified in the UACONF only after the macro run is completed.

```
Do you want to configure the RSA interface <Y>?
```

2. Enter **Y** to configure the service.

```
What is the TCP/IP process name <$ZTCP2>?
```

3. Enter your TCP/IP process name.

```
How many seconds should XUA wait for a RSA response before timeout occurs<30>?
```

4. Enter **30**.

```
Do you want to use RSA authentication for all NonStop users <No>?
```

5. Answer according to your need.

```
Do you want to require a password in addition to the SecurID token for all NonStop
users <NO>?
```

6. Answer according to your need.

```
Is your RSA server configured as a web service <N>?
```

7. Enter **Y**.

```
RSA Hostname?
```

8. Enter your RSA Authentication Service Domain as indicated in RSA Cloud Administration Console.

Example: rsa-demo.auth.securid.com

```
RSA access key?
```

9. Enter the **Authentication API Key** from the RSA Cloud Administration Console.

```
Enter unqualified CACERT filename?
```

10. Enter the name of a nonexistent file.

Example: RSACERT

Note: This value is not required because the certificate on RSA Cloud Authentication Service is already trusted.

```
RSA access ID?
```

11. Enter the RSA access ID

Note: This value is not used by RSA SecurID Access. XYPRO recommends to specify the email address of the person who configures this integration.

```
RSA Language?
```

12. Enter the language code.

Example: en_US

```
RSA Port <5555>?
```

13. Enter **443**.

```
RSA Path?
```

14. Enter **/mfa/v1_1**

RSA Security key type <KEY>?

15. Enter **KEY**

```
RSA Agent name?
```

16. Enter the name you wish to be displayed in the RSA Authenticate App's push notifications. Example notification: "Sign in request for: XUA"

```
RSA auth policy ID?
```

17. Enter the name of the access policy (as configured in RSA Cloud Administration Console) that XUA will use to authenticate users.

```
RSA Attempt timeout (seconds)?
```

18. Enter **120**. Increase this value if user authentications timeout before they can be completed.

```
Java install path </usr/tandem/nssjava/jdk180_h80>?
```

19. Enter the Java install path.

```
Do you want to configure the RSA interface now <Y>?
```

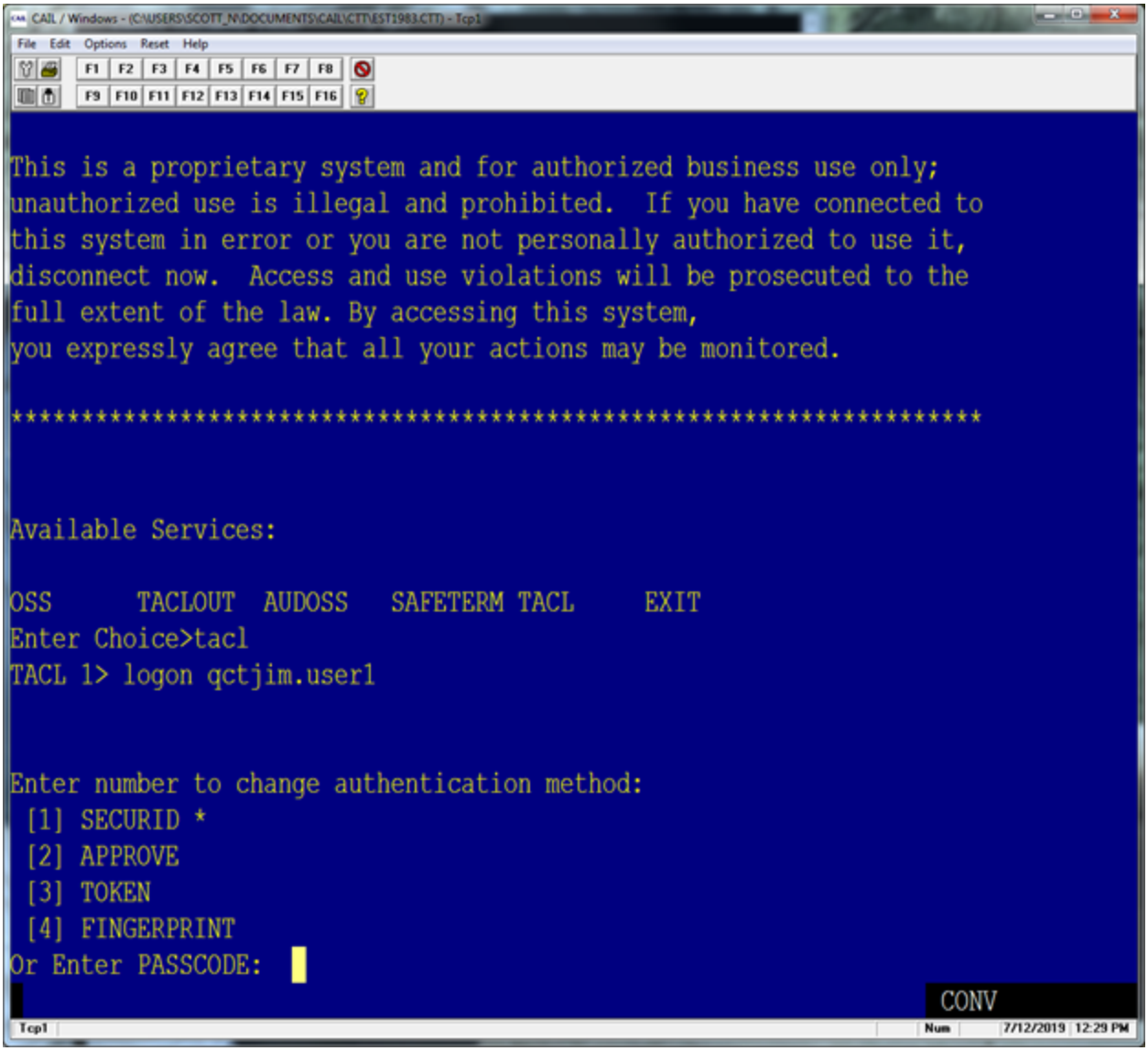
20. Enter **Y**.

Configuration is complete.

Note: Authenticating with the RSA SecurID Access requires the UAACL rule, UAGROUP, which maps NonStop user accounts to RSA user accounts and invokes RSA processing by XUA. Refer to XYGATE User Authentication Reference Manual for more information.

User Experience

Authentication method selection menu



Return to the main page for more certification related information.