



# Troubleshooting RSA SecurID Connections

## 10 Most Common User Issues

David Allison  
RSA Professional Services  
October 25, 2013

# Most Common Issues Using SecurID Tokens

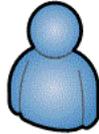
# What The User Should Be Doing

- To log in using a SecurID token, the user needs to present 3 pieces of information:
  - UserID
  - PIN
  - Tokencode
- Almost every logon failure is caused by the user not putting the right information in the right place

# What The User Should Be Doing

- For this presentation, we will use the following example:

– UserID



655321

– PIN

480420

– Tokencode



159759



# Sample Login Page

# Sample Login Page

**VPN PORTAL LOGIN**

User name:

PIN + Tokencode:



655321

PIN

480420



159759

# Correct Format



655321

PIN

480420



159759

<a href="#">i</a> <a href="#">2013-10-24 10:19:45.509</a>	Principal authentication	User "655321" attempted to authenticate using authenticator "SecurID_Native". The user belongs to security domain "SystemDomain"	Authentication succeeded in new PIN mode	655321
---	--------------------------	--	--	--------

# 1. Bad Tokencode, but Good PIN

VPN PORTAL LOGIN

User name:

PIN + Tokencode:



655321

PIN

480420



159759

 <a href="#">2013-10-24 10:27:24.062</a>	Authentication attempted	Bad tokencode, but good PIN detected for token serial number "000 [REDACTED]" assigned to user "655321" in security domain "SystemDomain" from "Internal Database(not used)" identity source	Authentication method failed	655321
---	--------------------------	---	------------------------------	--------

# 2. Bad Tokencode, but Good PIN

*(user is looking at the wrong token)*

**VPN PORTAL LOGIN**

User name:

PIN + Tokencode:



655321

PIN

480420



159759

 <a href="#">2013-10-24 10:27:24.062</a>	Authentication attempted	Bad tokencode, but good PIN detected for token serial number "000 [REDACTED]" assigned to user "655321" in security domain "SystemDomain" from "Internal Database(not used)" identity source	Authentication method failed	655321
---	--------------------------	---	------------------------------	--------

# 3. Bad Pin, But Good Tokencode



655321

PIN

480420



159759

 <a href="#">2013-10-24 10:28:44.312</a>	Authentication attempted	Bad PIN, but good tokencode detected for token serial number "000 [REDACTED]" assigned to user "655321" in security domain "SystemDomain" from "Internal Database(not used)" identity source	Authentication method failed	655321
---	--------------------------	---	------------------------------	--------

# 4. PIN and Tokencode Reversed



655321

PIN

480420



159759

 <a href="#">2013-10-24 10:17:16.127</a>	Principal authentication	User "655321" attempted to authenticate using authenticator "SecurID_Native". The user belongs to security domain "SystemDomain"	Authentication method failed, passcode format error	655321
---	--------------------------	--	---	--------

# 5. Principal (“user”) Locked Out



655321

PIN

480420



159759

 <a href="#">2013-10-24 10:31:38.888</a>	Principal authentication	User "655321" attempted to authenticate using authenticator "SecurID_Native". The user belongs to security domain "CustomDomain".	Principal locked out	655321
---	--------------------------	---	----------------------	--------

# 6. Principal Not Found

*(user ID and tokencode reversed)*



655321

PIN

480420



159759

 <a href="#">2013-10-24 10:25:44.405</a>	Principal authentication	User "159759" attempted to authenticate using authenticator "". The Principal not found 159759 user belongs to security domain ""	
---	--------------------------	---	--

# 7. Principal Not Found

*(adding domain credentials to user ID)*

## VPN PORTAL LOGIN

User name:

PIN + Tokencode:



655321

PIN

480420



159759

 <a href="#">2013-10-24 10:26:00.193</a>	Principal authentication	User "US-AD\655321" attempted to authenticate using authenticator "". The Principal not found user belongs to security domain ""	US-AD\655321
---	--------------------------	--	--------------

# 8. Principal Not Found

*(not separating user ID from passcode)*



VPN PORTAL LOGIN

User name: 655321159759

PIN + Tokencode:



655321

PIN

480420



159759

 <a href="#">2013-10-24 10:25:44.405</a>	Principal authentication	User "655321159759" attempted to authenticate using authenticator "". The Principal not found 655321159759 user belongs to security domain ""
---	--------------------------	---

# 9. Passcode Reuse Detected

*(each tokencode can only be used once)*



VPN PORTAL LOGIN

User name: 655321

PIN + Tokencode: 480420159759



655321

PIN

480420



159759

 <a href="#">2013-10-24 10:35:58.897</a>	Authentication attempted	Passcode reuse or previous token code detected for user "655321" in security domain "SystemDomain" from "Internal Database(not used)" identity source. Request originated from agent "" with IP address "" in security domain "" with protocol version "Internal Database(not used)". Authentication method: "SecurID_Native", Authentication policy exp: "SecurID_Native", Activation Group: "",	Authentication method failed	655321
---	--------------------------	---	------------------------------	--------

# 10. No Authenticator Assigned

VPN PORTAL LOGIN

User name: 655321

PIN + Tokencode: 480420159759



655321

PIN

480420



159759

 <a href="#">2013-10-24 10:37:22.02</a>	Principal authentication	User "655321" attempted to authenticate using authenticator "". The user belongs to security domain "SystemDomain"	Principal does not possess one or more authenticators	655321
--	--------------------------	--	---	--------

# In Summary

# Most Common Reasons for SecurID Login Failure

1. Good PIN but bad tokencode
2. Good PIN but bad tokencode – does the user have more than one token?
3. Good tokencode but bad PIN
4. Passcode format error - PIN and tokencode reversed; using PIN before one has been set; or space between PIN and tokencode
5. Principal (“user”) locked out
6. User not found in database – using tokencode instead of User ID
7. User not found in database – using domain credentials as part of User ID
8. User not found in database – using UserID and tokencode together in the same field
9. Passcode reuse detected – once a tokencode is used, it cannot be used again
10. No authenticator assigned – user is trying to log in but does not have a token

# Q&A



THANK YOU