[Duo MSP] Re: Duo MFA Questions

02/13/2024 12:52 pm EST

Subject	[Duo MSP] Re: Duo MFA Questions
From	Scott MacDonald (Duo MSP)
To	Jeff Mack
Sent	Friday, August 31, 2018 12:44 PM

##- Please type your reply above this line -##

Your request (1800496) has been updated. To add additional comments, reply to this email.

Scott MacDonald (Duo MSP)

Aug 31, 11:44 AM CDT

Hi Jeff,

Thanks for the information. In relation to your points:

1. When your New User Policy is set to "Allow access without 2FA," all users that are not listed under the Users page in your Duo Admin Panel will be allowed to authenticate without 2FA.

However, if a user exists but has no devices associated with them, this user is considered "partially enrolled." The user will be prompted to complete enrollment the next time they log in to an application with New User Policy set to "Allow access without 2FA," as long as that application supports inline self-enrollment. For applications that do not support the Duo Prompt, the user will be denied access, as there's no way to interactively prompt the user to complete enrollment.

For this reason, we suggest only performing a Bulk Enrollment or Directory Sync for users that you want to force to complete 2FA enrollment from the moment the sync or enrollment is performed.

Additionally, Group Access Policy overrides New User Policy. If there is a Group Access Policy that applies to a new user (not enrolled or partially enrolled), it will take precedence over the New User Policy.

2. Thank you for clarifying the situation. There is no connection between the RD Web and RDP application for Duo so they are not aware of each other presence and cannot communicate. This means that if someone logs into RD Web, they will get prompted for primary auth, then get prompted for secondary auth (Duo) and then once logged in and launch a connection to a host they will then go through the local Duo RDP prompts. I typically recommend to only install the Duo RDP plugin on the session host as it offers a more interactive experience.

3. Yes you are correct, A user who is bypassed is unable to enroll as they get bypassed from the enrollment process, to resolve this, set that user's status to "Active" and they will be able to self-enroll via the Duo Prompt.

Please let me know if you have any further questions.

Thanks

Scott

Jeff Mack

Aug 30, 2:12 PM CDT

1. Allow unenrolled users to pass through without two-factor authentication

2. Perhaps I didn't explain this situation well: we have customers set up to login via an RD Web portal (hosted on their application server; only a few customers with separate dedicated cloud systems have a separate RD Gateway with multiple RD Web servers). Most just use the RD Web site to login and access their apps through the browser. Some customers directly RDP to their application servers however, and we don't always know off hand which method they use to connect and access their applications. So we have our initial rollout customers' VMs running both Duo for RD Web and Duo for Windows/RDP Login. Our understanding of how Duo for RD Web works is that it would authenticate when they log into the portal site in their internet browser and then pass that to the remoteapp when they launched it. We had one case though where they got locked out of Duo because they weren't seeing the Duo authentication prompt for RDP/Windows login that came up when the remoteapp was connecting, because you'd have to had clicked the arrow to see details to see the Duo prompt on the remote screen. We've since allowed customers to remember devices for all applications for 1 day to theoretically resolve this kind of issue if the user checks the remember checkbox, but we wanted to know if that was the intended interaction between the two.

3. Sorry to spring another question on you, but is it correct that you cannot have a user in bypass status (whether from user or group) and have that user go through the enrolling via email? So is the intended process to set up and enroll users and then install the Duo software on the server?

Jeffery Mack

734-414-0760 x127

Scott MacDonald (Duo MSP)

Aug 30, 1:43 PM CDT

Hi Jeff,

Thanks for your email with questions on your duo deployment. To answer your questions I can confirm:

1. Can you confirm what your global policy is set to in terms of user enrollment?

2. If you place Duo on the RDWeb/RDGateway and on the host itself then the user should be required to complete the duo auth prompt twice. Duo offers no ability to offer secondary authentication to remote apps through RDWeb as we cannot intercept the url that is being called. More info can be found here: https://help.duo.com/s/article/1403?language=en_US

Please let me know if there are any other questions I can assist with.

Thanks

Scott

Craig Landreneau (Duo MSP)

Aug 30, 8:32 AM CDT

Hey Jeff,

Thank you for reaching out to us!

I am forwarding this ticket over to one of our SE's, who will be better equipped to answer your more technical questions.

You should be hearing back from us soon, but please let us know if you have any questions or concerns in the meantime!

Kind regards,

Craig Landreneau

Jeff Mack

Aug 29, 3:05 PM CDT

Hello,

We've started rolling out Duo MFA for some of our cloud customers and have a few more questions we'd like to clear up as we refine our process for rolling out Duo to customers.

First, we are using Active Directory Sync to bring in user groups so we can rollout customer-by-customer. We have been bringing in the users and then coordinating to send out enrollment emails. We have set the global new user policy to allow unenrolled users without MFA. It seems like we also need to set the groups we bring into AD to bypass until they are enrolled or else they get sent through the enrollment process upon logging in. Is this supposed to happen in spite of the new user policy? If so, is there a way we can set up Duo to deny anyone not added via AD Sync into Duo, but not force enrollment on the users we add?

The next question is how do RD Web and Windows/RDP Duo authentication interact when both are installed on one server? We had one user claim they got passed Duo to the RD Web portal, but were unable to access their remote apps. When I connected with them, I saw there was a Duo prompt for RDP hidden in the details for connecting to the remote app. This was meant to automatically send a Duo Push to them, but I believe they did not have or did not understand Push at the time as they authenticated to RD Web via call. So they had actually locked themselves out in Duo as of the first attempt when I was connected to assist. We unlocked them and got them logged into their app, but I want to make sure I understand how RD Web and RDP Duo Authentication will interact if both are installed on the same server. Of our RD Web customers, some use RD Web and others don't even use RD Web and just RDP into the server. So ideally we would like both on the same server.

And I'll probably find this answer in documentation or just testing myself before I hear back, but I just wanted to double-check that if we set the policy so users can remember devices, this presents the end user with a checkbox to remember the device (i.e. it's optional). Some users want to be prompted every time and others do not.

Jeff Mack

IT Support Specialist

Perennial Software

(734) 414-0760 x127