

Risk check actions

The following table describes the types of failure actions to take when the end user does not meet the adaptive authentication risk check requirements.

Action	Result
Continue Adaptive Authentication	Continue with the next adaptive authentication risk check When all adaptive authentication risk checks are completed, the end user is taken through the workflow steps.
Refuse authentication request	Immediately block the login request Stops all workflows, remaining adaptive authentication risk checks, and post authentication actions.
Skip to post-authentication	Move the end user to the post-authentication target Exits the adaptive authentication risk checks. The end user continues to the post authentication target (such as Identity Management page or application) and bypasses all workflows and remaining adaptive authentication risk checks and a password check, if the workflow is configured for this.
Redirect to realm or URL	Redirects the end user to another URL Exits the adaptive authentication risk checks and redirects the end user to alternate URL or realm as defined in the text field. The end user continues with the alternate workflow and bypasses other workflows and remaining adaptive authentication risk checks.
Resume authentication workflow	Move the end user to the next workflow step Exits the adaptive authentication risk checks. The end user continues to the next step in the workflow with a persistent token check or two-factor authentication.
Skip two-factor authentication	Move the end user to the next workflow step, bypassing additional adaptive authentication risk checks and two-factor authentication Exits the adaptive authentication risk checks. The end user is taken to the next workflow step (which might require them to enter a password) and bypasses remaining adaptive authentication risk checks, persistent token check, and two-factor authentication check. <div style="background-color: #ffffcc; padding: 10px; margin-top: 10px;"> <p>If you do not see this option when configuring your two-factor authentication settings in the Adaptive Authentication section, be sure you have selected a default workflow that includes second factor on the Workflow tab.</p> </div>
Require two-factor authentication	Requires two-factor authentication Exits the adaptive authentication risk checks. The end user continues through the workflow using two-factor authentication; and bypasses the persistent token check such as device recognition / fingerprint, cookie, or certificate. <div style="background-color: #ffffcc; padding: 10px; margin-top: 10px;"> <p>If you do not see this option when configuring your two-factor authentication settings in the Adaptive Authentication section, be sure you have selected a default workflow that includes second factor on the Workflow tab.</p> </div>