
Policy Directive: Ping Deploy Confidentiality

Ping Deploy provides conformance testing information to businesses dependent on identity federation protocols. This information is obtained either through a mediated, web-accessible testing service or through the staging of tests in Ping Identity's labs or on the client's premises.

This policy recognizes that all testing produces information that is considered business sensitive. Further, it is understood that it is the responsibility of those involved in providing the testing service to hold all information related to the setup, test configurations, and test results confidential. Confidentiality must be maintained on two fronts: 1) From those external, much as we guard and hold confidential our proprietary information and 2) From anyone not directly involved in the testing process. Consistent with that, the following standards will be upheld:

- All Ping Deploy customer engagements require the execution of Ping Identity's standard NDA or similar provided by the customer.
- All information related to testing, including but not limited to test configurations and results, will be held in a confidential way with conversations restricted to the Conformance Engineer and customer.
- All test engagements will be conducted under a code name that masks the customer's name. This code name will be issued by accounting to the Conformance Engineer on receipt of a purchase order. All dialogs, written or spoken, will utilize the code name with no reference made to the customer company name. All time reporting will utilize the code name.
- Should a situation arise where there are divergent interpretations of the specification between a vendor implementation and the approved script pack of the Conformance Working Group, Ping Identity will work with the customer to understand and document the vendor interpretation. If requested by the vendor, a Ping Identity representative will present the alternative interpretation in a meeting of the SAML Conformance Working Group members, without disclosing the name of the company to obtain a formal ruling on the interpretation(s) under question. In this way, customers of the testing service will be able to resolve potential interpretation issues with the Conformance Working Group while maintaining the confidentiality of their test results.
- All conversations during testing situations will be conducted from a private lab with a door. This lab will be considered off limits to all members of the product development effort during all setup and testing activities.
- Individuals who provide the mediation of the Ping Deploy conformance testing service and who are directly involved with the customer test information and summary results will not be involved in the requirements specification, design, or implementation of any Ping Federate software. The Conformance Engineer may act in a role as an independent tester of Ping Federate software much as might be done for an external customer.
- Should a situation arise where more than the Conformance Engineer is required to resolve issues with a test or test software, the details will only be shared on a need to know basis and only with an individual assigned to Ping Deploy sustaining engineering. All such situations will be logged to the Ping Deploy chronological journal.
- Access restrictions will be applied to customer configuration definition, administration of test setup and execution, access to all test logs and results. All servers involved in providing Ping Deploy service will operate under password protection with access limited to Ping Deploy Conformance Engineers and those in IT responsible for daily maintenance/backup.
- All test results and related information, raw and summary, will be scrubbed from all active storage. All raw and summary information will be written to optical storage with the media held in a limited-access, fire-proof lock box.
- Ping Identity's Compliance Officer will conduct an annual audit to the points above. A report with a corrective action plan, if needed, will be issued to me within two weeks of the audit.

This directive is immediately active on general availability of the Ping Deploy conformance testing service.



Andre Durand, CEO
Ping Identity