
DOYENSEC
Teleport

DOYENSEC'S
Teleport IdP Hardening Checklist

Protect your cluster, even if your IdP is compromised!

Doyensec has drafted a checklist to verify whether your Teleport cluster has all the available protections and best practices in place to enhance security against IdP compromise scenarios.

- ☐ **Just-in-time Access Requests** is configured according to the least-privilege principle; Request reviewers are only local users (i.e., No SSO users as reviewers);
- ☐ **Dual-Authorization** is set to further restrict access to administrative actions and implement the concept of ephemeral administrators. Requests reviewers are only local users (i.e., No SSO users as reviewers);
- ☐ **SSO Connectors (IdPs)** are configured to **restrict roles mappings and automatic provisioning** capabilities from non-admin IdP users
  - ☐ The username field (IdP-side) mapped as Teleport username is not editable by end-users and is unique in the IdP's users pool;
  - ☐ The group field (IdP-side), used to map roles in Teleport, is editable by a very restricted group of users in the IdP and is unique in the organization;
  - ☐ The Teleport SSO Connector does not apply lax string matching to map roles. Instead, fixed values from the IdP group are mapped to roles;
- ☐ **Device Trust** can be configured to **protect against new SSO users** being auto-provisioned from a compromised IdP. By enforcing it, new SSO users need to perform the **first MFA device enrollment** from a trusted device;
- ☐ **Access Lists** granting administrative permissions **(see RFD 131 [11]) do not have:**
  - ☐ **SSO identities.** Only local users should obtain high privileges via access list;
  - ☐ **Implicit rules referencing attributes obtained from the SSO source;**
  - ☐ **Dangling Identities** which are no longer part of the cluster;
- ☐ An **additional Identity Confirmation Layer** is applied
  - ☐ **Per-session MFA** is applied cluster-wide to restrict access to various resources with MFA devices;
  - ☐ **WebAuthn** is forced as second factor to avoid OTP-related attacks;
  - ☐ **Administrative Actions MFA Requirement** is active for admin actions, with MFA challenges;
- ☐ **Detection & Incident Response Strategies** are in place
  - ☐ There are watchdogs listening on the valuable events emitted by Teleport (Please refer to the detection section of each threat analyzed in this paper to build custom rules);
  - ☐ **Moderated Sessions** admins are configured as local users, ready to join or assess suspicious sessions;
  - ☐ Admins with SSO Connectors management and locking capabilities are ready to be used to block new malicious sessions or invalidate existing ones;
- ☐ **Teleport roles do not reference external values** taken from the IdP mappings.