Oracle Platinum Services – Remote Access Control

Inbound Access Requirements

ORACLE
PREMIER SUPPORT

Contents

Document Objective

The objective of this document is to:

- Outline some of the common reasons Oracle requires inbound access to the gateway and customer's Certified Platinum Configuration,
- Outline Oracle's current process, which is subject to change, for requesting inbound access, and
- Provide expectations of customer response time to inbound access requests.

Overview

The Platinum Remote Access Control feature of the Advanced Support Gateway (gateway) allows enabling / disabling of the Secure Sockets Layer (SSL) Virtual Private Network (VPN) connection via Command Line Interface. Disabling the SSL VPN prevents Oracle from inbound access to the gateway and the Certified Platinum Configuration. Oracle requires periodic inbound access to the Gateway and the Certified Platinum Configuration to provide both reactive and proactive Platinum Support Services.

- Oracle's ability to perform the Platinum Support Services is contingent upon the SSL VPN connection to the gateway being enabled. Please review the Oracle Platinum Services Technical Support Policy at http://www.oracle.com/us/support/library/platinum-services-policies-1652886.pdf.
- A list of Certified Platinum Configurations is available at http://www.oracle.com/us/support/library/certified-platinum-configs-1652888.pdf.

Note the Remote Access Control feature is not available to customers with an Internet Protocol Security (IPSec) VPN configuration.

Common Inbound Access Requirements

Gateway and Monitoring Agents – Diagnosis and Resolution

Oracle commonly requires inbound access to diagnose and resolve gateway and monitoring agent issues, and for reactive system administration issues on the gateway. Activities include, but are not limited to:

- Resolving monitoring heartbeat failures
- Restarting monitoring components
- Restarting failed monitoring agents
- Resolve disk space issues

Gateway and Monitoring Agents – Proactive Support

Oracle commonly requires inbound access proactively to manage the gateway and monitoring agents. Activities include, but are not limited to:

- Monitoring software and monitoring agent upgrades
- Operating System upgrades
- Patching
- Password administration

Gateway – Emergency Patching

Oracle periodically requires inbound access to the gateway for patching deemed to be an emergency. This may include, but is not limited to patching for:

- Critical security vulnerabilities that may impact the customer and Oracle
- Critical gateway software bugs that may impact delivery of Oracle Platinum Services

Customer Service Request – Diagnosis and Resolution

Oracle commonly requires inbound access to the Certified Platinum Configuration to aid in Service Request diagnosis and resolution. Activities include, but are not limited to:

- Retrieving log files
- Retrieving trace files
- Retrieving configuration files

Proactive Patch Deployment on the Certified Platinum Configuration

Oracle requires inbound access to the Certified Platinum Configuration for the Oracle Platinum Services Remote Patch Deployment Service. For more information see the Remote Patch Deployment "What to Expect" document located at http://www.oracle.com/us/support/library/platinum-remote-patch-checklist-1958298.pdf.

Access Request Process

If the SSL VPN connection is disabled, Oracle must request access to the gateway and Certified Platinum Configuration to perform proactive maintenance and respond reactively to issues. Oracle will use the customer contact telephone or e-mail information it has on file to request access. It is customer's obligation to ensure such contact information is up to date and the customer contact has the authority to reestablish SSL VPN connectivity to the gateway and the Certified Platinum Configuration.

Upon requesting access, Oracle may require a security vulnerability scan on the gateway, as well as other assurance and remediation processes as determined necessary by Oracle, prior to resumption of the Platinum Support Service. A Service Request will be opened and reference why access to the gateway and/or the Certified Platinum Configuration is being requested. The customer should update the Service Request once SSL VPN connectivity is restored. Failure to respond or reestablish SSL VPN connectivity promptly may lead to delays in the provision of Platinum Support Services, including but not limited to issue resolution or service restoration.