

Executing Host Checker Policies

When the user tries to access the Infranet Controller, Host Checker evaluates its policies in the following order:

1. **Initial evaluation**—When a user first tries to access the Infranet Controller sign-in page, Host Checker performs an initial evaluation. Using the rules you specify in your policies, Host Checker verifies that the client meets your endpoint requirements and returns its results to the Infranet Controller. Host Checker performs an initial evaluation regardless of whether you have implemented Host Checker policies at the realm, role, or resource policy level.

For agentless access deployments, if the user navigates away from the Infranet Controller sign-in page after Host Checker starts running but before signing in to the Infranet Controller, Host Checker continues to run on the user's machine until the Host Checker process times out. If the Infranet Controller does not receive a result from Host Checker for any reason (including because the user manually terminated Odyssey Access Client or Host Checker), the Infranet Controller displays the remediation instructions if they are enabled, or else displays an error and directs the user back to the sign-in page.

Otherwise, if the Host Checker process returns a result, the Infranet Controller goes on to evaluate the realm-level policies.

2. **Realm-level policies**—The Infranet Controller uses the results from Host Checker's initial evaluation to determine which realms the user may access. Then, the Infranet Controller displays or hides realms from the user, only allowing him to sign into those realms that you enable for the sign-in page, and if he meets the Host Checker requirements for each realm. If the user cannot meet the Host Checker conditions required by any of the available realms, the Infranet Controller does not display the sign-in page. Instead, it displays an error stating the user has no access unless you configure remediation actions to help the user bring his computer into compliance.



NOTE: The Host Checker performs realm-level checks when the user first signs into the Infranet Controller and during the user's session.

3. **Role-level policies**—After the user signs into a realm, the Infranet Controller evaluates role-level policies and maps the user to the role or roles if he meets the Host Checker requirements for those role(s). Then, the Infranet Controller pushes the role and policy information to the Infranet Enforcer and Odyssey Access Client.

If Host Checker returns a different status during a periodic evaluation, the Infranet Controller dynamically remaps the user to roles based on the new results. If the user loses rights to all available roles during one of the periodic evaluations, the Infranet Controller disconnects the user's session unless you configure remediation actions to help the user bring his computer into compliance.

4. **Infranet Enforcer resource access policies and Host Enforcer policies**—After the Infranet Controller pushes the role and policy information to the Infranet Enforcer and Odyssey Access Client, the user may try to access a protected resource that is controlled by an Infranet Enforcer resource access policy or Host

Enforcer policy. When he does, the Infranet Enforcer or Odyssey Access Client determines whether or not to allow or deny the user access to the protected resource based on the user's assigned role.

If Host Checker returns a different status during a periodic evaluation, the new status can change the assigned roles. The Infranet Controller then pushes the role and policy information to the Infranet Enforcer and Odyssey Access Client, which could prevent the user from accessing the protected resource.

With either a success or failure, Odyssey Access Client or Host Checker remains on the client. Windows users can manually uninstall Odyssey Access Client from the control panel.

If you enable client-side logging through the Infranet Controller, then the directory where Odyssey Access Client is installed contains a log file, which the Infranet Controller appends each time Odyssey Access Client or Host Checker runs.

You may specify that the Infranet Controller evaluate your Host Checker policies only when the user first tries to access the realm or role that references the Host Checker policy. Or, you may specify that the Infranet Controller periodically reevaluate the policies throughout the user's session. If you choose to periodically evaluate Host Checker policies, the Infranet Controller dynamically maps users to roles and instructs the Infranet Enforcer or Odyssey Access Client to allow users access to new resources based on the most recent evaluation.

Use a Host Checker restriction to require client machines to meet the specified Host Checker policies to access an Infranet Controller sign-in page or be mapped to a role.

- Related Topics**
- Implementing Infranet Controller Host Checker Policies (NSM Procedure)
 - Remediating Infranet Controller Host Checker Policies