

Implementing Infranet Controller Host Checker Policies (NSM Procedure)

Implementing Infranet Controller Host Checker policies involves:

- Restricting Infranet Controller and Resource Access Through Host Checker on page 1
- Configuring Host Checker Restrictions on page 2

Restricting Infranet Controller and Resource Access Through Host Checker

After you create global policies, you can restrict Infranet Controller and resource access through the Host Checker in a policy or role:

Realm authentication policy—When administrators or users try to sign in to the Infranet Controller, the Infranet Controller evaluates the specified realm's authentication policy to determine if the preauthentication requirements include Host Checker. You can configure a realm authentication policy to download Host Checker, launch Host Checker, and enforce Host Checker policies specified for the realm, or not require Host Checker. The user must sign in using a computer that adheres to the Host Checker requirements specified for the realm. If the user's computer does not meet the requirements, then the Infranet Controller denies access to the user unless you configure remediation actions to help the user bring his computer into compliance.

To configure realm-level restrictions:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to realm-level restrictions.
3. Click the **Configuration** tab. In the configuration tree,
 - select **Administrators > Admin Realms > Select Realm > Authentication Policy > Host Checker** to configure administrator realm-level restrictions.
 - select **Users > User Realms > Select Realm > Authentication Policy > Host Checker** to configure user realm-level restrictions.
4. Configure realm-level restrictions.
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Role—When the Infranet Controller determines the list of eligible roles to which it can map an administrator or user, it evaluates each role's restrictions to determine if the role requires that the user's computer adheres to certain Host Checker policies. If it does and the user's computer does not follow the specified Host Checker policies, then the Infranet Controller does not map the user to that role unless you configure remediation actions to help the user bring his computer into compliance.

To configure role-level restrictions:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to role-level restrictions.
3. Click the **Configuration** tab. In the configuration tree,
 - select **Administrators > Admin Roles > Select Role > General > Restrictions** to configure administrator role-level restrictions.
 - select **Users > User Roles > Select Role > General > Restriction** to configure user role-level restrictions.
4. Configure role-level restrictions.
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Configuring Host Checker Restrictions

To configure Host Checker restrictions:

1. Specify global Host Checker restrictions. See “Creating Infranet Controller Global Host Checker Policies (NSM Procedure).”
2. If you want to implement Host Checker at the *realm* level and *role* level, see “Configuring Infranet Controller Host Checker Access Restrictions (NSM Procedure).”
3. If you want to create role-mapping rules based on a user’s Host Checker status, see “Configuring Role Mapping Rules (NSM Procedure).”

- Related Topics**
- Remediating Infranet Controller Host Checker Policies
 - Executing Host Checker Policies