Portal Settings for Client Provisioning Portals

Portal Settings

- **HTTPS Port**: Enter a port value between 8000 to 8999; the default value is 8443 for all the default portals, except the **Blacklist** Portal, which is 8444. If you upgraded with port values outside this range, they are honored until you make any change to this page. If you make any change to this page, you must update the port setting to comply with this restriction.
- **Allowed Interfaces**: Select the PSN interfaces which can run a portal. Only a PSN with an available allowed interface on a PSN can create a portal. You can configure any combination of physical and bonded interfaces. This is a PSN-wide configuration; all portals can only run on these interfaces, this interface configuration is pushed to all the PSNs.
  - You must configure the Ethernet interfaces using IP addresses on different subnets.
  - The interfaces you enable here must be available on all your PSNs, including VM-based ones when Policy Services turned on. This is required because any of these PSNs can be used for a redirect at the start of the guest session.
  - The portal certificate Subject Name/Alternate Subject Name must resolve to the interface IP.
  - Configure ip host x.x.x.x yyy.domain.com in ISE CLI to map secondary interface IP to FQDN, which will be used to match Certificate Subject Name/Alternate Subject Name.
  - If only the bonded NIC is selected, when the PSN attempts to configure the portal it first attempts to configure the Bond interface. If that is not successful, perhaps because there was no bond set upon that PSN, then the PSN logs an error and exits. It will NOT attempt to start the portal on the physical interface.
  - **NIC Teaming** or bonding is an O/S configuration option that allows you to configure two individual NICs for high availability (fault tolerance). If one of the NICs fails, the other NIC that is part of the bonded connection continues the connection. A NIC is selected for a portal based on the portal settings configuration:
    - If both physical NICs and the corresponding bonded NIC are configured - When the PSN attempts to configure the portal, it first attempts to connect to the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN attempts to start the portal on the physical interface.
- **Certificate Group Tag**: Select the group tag of the certificate group to use for the portal's HTTPS traffic.

- **Authentication Method**: Choose which identity source sequence (ISS) or Identity Provider (IdP) to use for user authentication. The ISS is a list of Identity Stores that are searched in sequence to verify user credentials. Some examples include: Internal Guest Users, Internal Users, Active Directory, and LDAP.

  Cisco ISE includes a default client provisioning Identity Source Sequence for Client Provisioning Portals, Certificate_Request_Sequence.

- **Fully Qualified Domain Name (FQDN)**: Enter at least one unique FQDN and/or hostname for your Client Provisioning portal. For example, you can enter provisionportal.yourcompany.com, so that when the user enters either of those into a browser, they will reach the Client Provisioning Portal.

  - Update DNS to ensure that the FQDN of the new URL resolves to a valid Policy Services Node (PSN) IP address. Optionally, this address could point to a load balancer virtual IP address that serves a pool of PSNs.
  - To avoid certificate warning messages due to name mismatches, include the FQDN of the customized URL, or a wildcard, in the subject alternative name (SAN) attribute of the local server certificate of the Cisco ISE PSN.

Note For Client Provisioning without URL redirection, the portal name that is entered in the Fully Qualified Domain Name (FQDN) field must be configured in the DNS configuration. This URL must be communicated to the users to enable Client Provisioning without URL redirection.

- **Idle Timeout**: Enter the time in minutes that you want Cisco ISE to wait before it logs out the user if there is no activity in the portal. The valid range is from 1 to 30 minutes..

Note In the Client Provisioning Portal, you can define the port number and the certificate so that the host allows you to download the same certificate for Client Provisioning and Posture. If the portal certificate is signed by the officials certificate authority, you will not receive any security warning. If the certificate is self-signed, you will receive one security warning for both the portals and Cisco AnyConnect Posture component.

Login Page Settings

- Enable Login: Select this check box to enable the login step in the Client Provisioning Portal
- Maximum failed login attempts before rate limiting: Specify the number of failed login attempts from a single browser session before Cisco ISE starts to artificially slow down the rate at which login attempts can be made, preventing additional login attempts. The time between attempts after this number of failed logins is reached is specified in **Time between login attempts when rate limiting**.
- Time between login attempts when rate limiting: Set the length of time in minutes that a user must wait before attempting to log in again, after failing to log in the number of times defined in **Maximum failed login attempts before rate limiting**.
- Include an AUP (on page/as link): Display your company's network-usage terms and conditions, either as text on the page currently being displayed for the user or as a link that opens a new tab or window with AUP text.

- Require acceptance: Require users to accept an AUP before they can access the portal. The **Login** button is not enabled unless the user accepts the AUP. If users do not accept the AUP, they will not be able to access the portal.
- Require scrolling to end of AUP: This option displays only if **Include an AUP on page** is enabled. Ensure that the user has read the AUP completely. The **Accept** button activates only after the user has scrolled to the end of the AUP.

Acceptable Use Policy (AUP) Page Settings

- Include an AUP: Display your company's network-usage terms and conditions on a separate page to the user.
- Require scrolling to end of AUP: Ensure that the user has read the AUP completely. The Accept button activates only after the user has scrolled to the end of the AUP.
- On first login only: Display an AUP when the user logs into the network or portal for the first time only.
- On every login: Display an AUP each time the user logs into the network or portal.
- Every _____ days (starting at first login): Display an AUP periodically after the user first logs into the network or portal.

Post-Login Banner Page Settings

Include a Post-Login Banner page: Display additional information after the users successfully log in and before they are granted network access.

Change Password Settings

Allow internal users to change their own passwords: Allow employees to change their passwords after they log in to the Client Provisioning Portal. This only applies to employees whose accounts are stored in the Cisco ISE database and not to those stored in external databases, such as Active Directory or LDAP.

- HTML Support for Client Provisioning Portal Language Files, on page 3

HTML Support for Client Provisioning Portal Language Files

The navigation path to this portal's **Instructional Text** , **Content**,**Optional Content 1**, and **Optional Content 2** text boxes is **Administration** > **Device Portal Management** > **Client Provisioning Portals** > **Edit** > **Portal Page Customization** > **Pages**. You can use the **View HTML Source** icon in the mini-editor and add HTML code in your content.

These dictionary keys in the portal's language properties files support HTML in their text.

Note This is not a complete list of the dictionary keys in the files.

- key.guest.ui_client_provision_agent_installed_instructions_without_java_message
- key.guest.ui_contact_instruction_message
- key.guest.ui_success_message

- key.guest.ui_client_provision_unable_to_detect_message
- key.guest.ui_client_provision_instruction_message
- key.guest.ui_client_provision_agent_installation_message
- key.guest.ui_client_provision_posture_agent_check_message
- key.guest.ui_vlan_instruction_message
- key.guest.ui_client_provision_agent_installation_instructions_with_no_java_message
- key.guest.ui_success_instruction_message
- key.guest.ui_vlan_optional_content_1
- key.guest.ui_vlan_optional_content_2
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1
- key.guest.ui_contact_optional_content_1
- key.guest.ui_client_provision_posture_check_compliant_message
- key.guest.ui_client_provision_optional_content_2
- key.guest.ui_client_provision_optional_content_1
- key.guest.ui_error_optional_content_2
- key.guest.ui_error_optional_content_1
- key.guest.ui_client_provision_posture_check_non_compliant_message
- key.guest.ui_vlan_install_message
- key.guest.ui_success_optional_content_1
- key.guest.ui_success_optional_content_2
- key.guest.ui_client_provision_posture_agent_scan_message