



CHAPTER 6

Configuring Guest Login Policies

Organizations commonly have policies in place for creating accounts for their internal users and systems, such as the format or length of the username and/or complexity of password. The Cisco NAC Guest Server allows you to configure guest username and password creation policies to match your organization's policy or to create a policy specific to guest accounts.

Setting the Username Policy

The Username Policy determines how to create user names for all guest accounts.

- Step 1** From the administration interface, select **Guest Policy > Username Policy** from the left hand menu (Figure 6-1).

Figure 6-1 Guest Username Policy

Username Policy Option 1

Use email address as username

Username Policy Option 2

Create username based upon first and last names

Minimum Username Length: 10

Username Policy Option 3

Create random username

Alphabetic Characters

Characters to include: ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz

Number to include: 6

Numeric Characters

Characters to include: 1234567890

Number to include: 1

Other Characters

Characters to include: !@#\$%*?

Number to include: 0

188317

Set Policy Reset Form

Step 2 Choose one of three options for creating the user name for the guest account.

- **Username Policy 1 (email)**

Use the guest's email address as the username. If an overlapping account with the same email address exists, a random number is added to the end of the email address to make the username unique. Overlapping accounts are accounts that have the same email address and are valid for an overlapping period of time.

- **Username Policy 2 (FirstLast)**

Create a username based on combining the first name and last name of the guest. You can set a Minimum Username Length for this username from 10 to 20 characters (default is 10). User names shorter than the minimum length are padded up to the minimum specified length with a random number.

- **Username Policy 3 (Random)**

Create a username based upon a random mixture of Alphabetic, Numeric or Other characters. Type the characters to include to generate the random characters and the number to use from each set of characters.



Note The total length of the username is determined by the total number of characters included.

Step 3 When done, click **Set Policy** to have the username policy take effect.

Setting the Password Policy

The password policy determines how to create the password for all guest accounts.

Step 1 From the administration interface, select **Guest Policy > Password Policy** from the left hand menu ([Figure 6-2](#)).

Figure 6-2 Password Policy

Alphabetic Characters

Characters to include: ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz

Number to include: 6

Numeric Characters

Characters to include: 1234567890

Number to include: 2

Other Characters

Characters to include: !@#\$%*

Characters to include: 0

185302

Set Policy Reset Form

- Step 2** In the **Alphabetic Characters** section, enter the characters to use in the password and the amount to include.
- Step 3** In the **Numeric Characters** section, enter the numerals to use in the password and the amount to include.
- Step 4** In the **Other Characters** section, enter the special characters to use in the password and the amount to include.

**Caution**

For passwords, use only the following characters for the “Other Characters” field: ! \$ ^ & * () - _ = + [] { } ; : @ # ~ , > ?.

Do **not** use the following characters in the “Other Characters” field, as they are **not** supported by the Clean Access Manager API: £ % < ¬ ` ' \ |.

- Step 5** Click **Set Policy** to save the settings.

**Note**

The total length of the password is determined by the total number of characters included. You can choose between 0 and 20 characters per type (alphabetic, numeric, or other).

