



Preparing for the Installation

This section includes the following topics:

- [Information Required for Configuration and Installation, page 1](#)
- [Shared Secret Password Criteria, page 2](#)
- [Configuring Chrome for Use with Prime Network Services Controller, page 3](#)

Information Required for Configuration and Installation

Before installation, collect the following information:

Required Information	Your Information/Notes
For Preinstallation Configuration	
ISO or OVA image location	
ISO or OVA image name	
Network / Port Profile for VM management ¹	
VM / Instance name	
KVM flavor name	
KVM Instance Security Group	
VMware datastore location	
For Prime Network Services Controller Installation	
IP address For OpenStack environments, use the IP address that is assigned to the Prime Network Services Controller instance in OpenStack.	

Required Information	Your Information/Notes
Subnet mask	
Hostname	
Domain name	
Gateway IP address	
DNS server IP address	
NTP server IP address	
Admin password	
Shared secret password for communication between Prime Network Services Controller and managed VMs. (See Shared Secret Password Criteria , on page 2.)	

¹ The management port profile is the same port profile that is used for Cisco Virtual Supervisor Module (VSM). The port profile is configured in VSM and used for the Prime Network Services Controller management interface.

Shared Secret Password Criteria

A shared secret password is a password that is known to only those using a secure communication channel. Passwords are designated as strong if they cannot be easily guessed for unauthorized access. When you set a shared secret password for communications between Prime Network Services Controller, VSG, ASA 1000V, and VSM, adhere to the following criteria for setting valid, strong passwords:

- Do not include special characters or spaces.
- Make sure your password contains the characteristics of strong passwords and avoids the characteristics of weak passwords as described in the following table:

Strong Passwords	Weak Passwords
<ul style="list-style-type: none"> • At least eight characters. • Contain characters from at least three of the following classes: lowercase letters, uppercase letters, and numbers. 	<ul style="list-style-type: none"> • Consecutive alphanumeric characters, such as <i>abcd</i> or <i>123</i>. • Characters repeated three or more times, such as <i>aaabbb</i>. • A variation of the word <i>Cisco</i>, such as <i>cisco</i>, <i>ocsic</i>, or one that changes the capitalization of letters in the word <i>Cisco</i>. • The username or the username in reverse. • A permutation of characters present in the username or <i>Cisco</i>.

Examples of strong passwords are:

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21
- Es1955Ap

Configuring Chrome for Use with Prime Network Services Controller

To use Chrome with Prime Network Services Controller, you must disable the Adobe Flash Player plugins that are installed by default with Chrome.



Note Because Chrome automatically enables Adobe Flash Player plugins each time the system reboots, you must perform this procedure each time your client machine reboots.

Procedure

- Step 1** In the Chrome URL field, enter **chrome://plugins**.
- Step 2** Click **Details** to expand all the files associated with each plugin.
- Step 3** Locate the Adobe Flash Player plugins, and disable each one.
- Step 4** Download and install Adobe Flash Player plugin version 11.9 or higher.
- Step 5** Close and reopen Chrome before logging in to Prime Network Services Controller.

