

Omnia 1.4

Security Configuration Guide

Notes, cautions, and warnings

 **NOTE:** A NOTE indicates important information that helps you make better use of your product.

 **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

 **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

Chapter 1: Preface	4
Legal disclaimers	5
Scope of the document	5
Document references	5
Reporting security vulnerabilities	5
Follow us online	5
Chapter 2: Security Quick Reference	6
Security profiles	6
Chapter 3: Product and Subsystem Security	7
Security controls map	7
Authentication	8
Cluster authentication tool	8
Authentication types and setup	8
Login security settings	8
User and credential management	9
Root user	9
Other users	9
Authentication to external systems	9
Deployment model	9
Network security	9
Network exposure	9
Data security	12
Auditing and logging	12
Logs	12
Logging format	12
Chapter 4: Miscellaneous Configuration and Management Elements	13
Licensing	13
Protect authenticity	13
Ansible security	14
Ansible vault	14

Preface

The security configuration guide of Omnia provides Dell customers an overview and understanding of the security features supported by Omnia 1.4. As part of an effort to improve its product lines, Dell periodically releases revisions of its software and hardware. The product release notes provide the most up-to-date information about product features. Contact your Dell technical support professional if a product does not function properly or does not function as described in this document. This document was accurate at publication time. To ensure that you are using the latest version of this document, go to [Omnia: Docs](#).

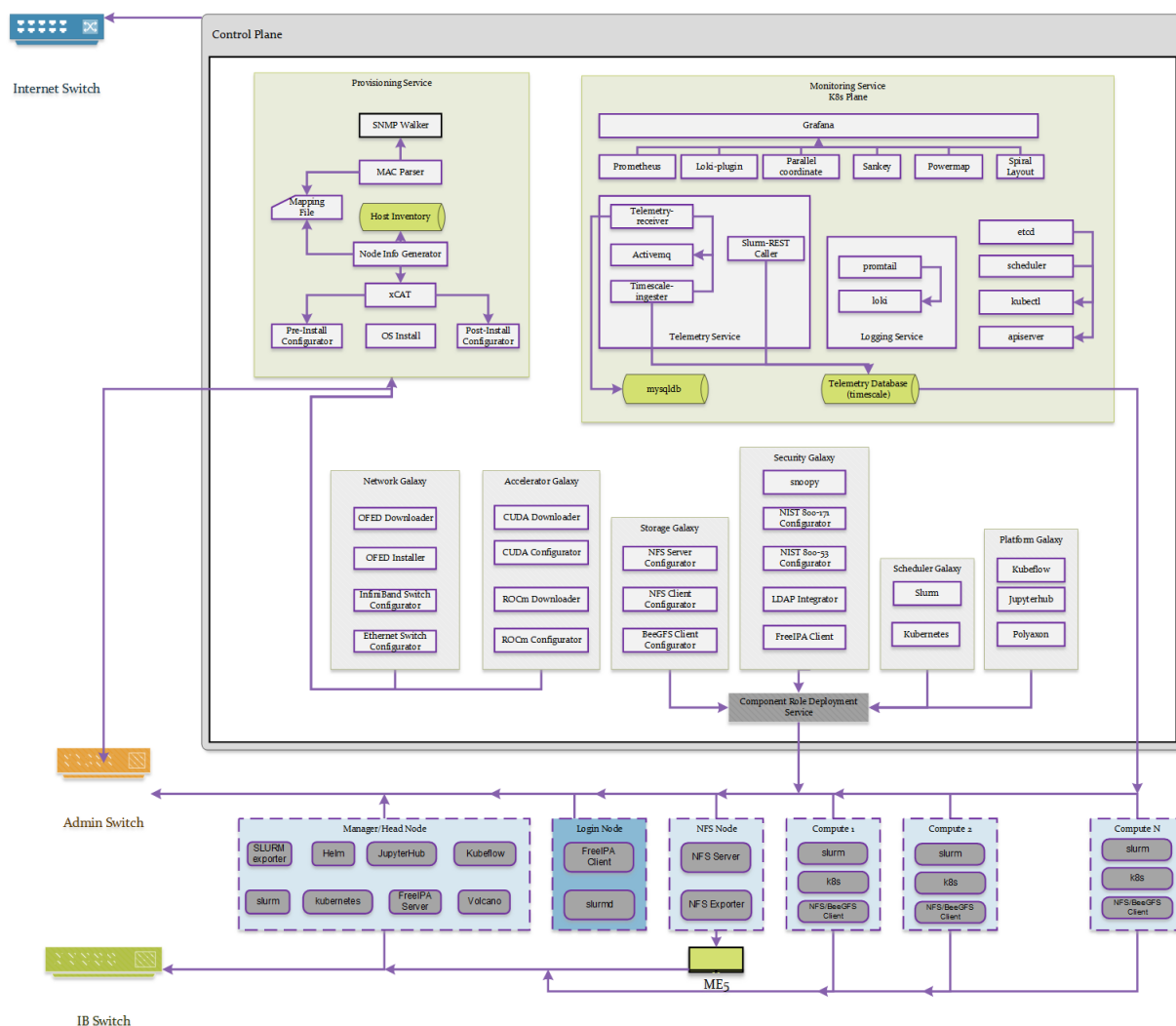


Figure 1. Typical layout of the HPC Cluster

Topics:

- [Legal disclaimers](#)
- [Scope of the document](#)
- [Document references](#)
- [Reporting security vulnerabilities](#)
- [Follow us online](#)

Legal disclaimers

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS-IS." DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. In no event shall Dell Technologies, its affiliates or suppliers, be liable for any damages whatsoever arising from or related to the information contained herein or actions that you decide to take based thereon, including any direct, indirect, incidental, consequential, loss of business profits or special damages, even if Dell Technologies, its affiliates or suppliers have been advised of the possibility of such damages.

The Security Configuration Guide intends to be a reference. The guidance is provided based on a diverse set of installed systems and may not represent the actual risk/guidance to your local installation and individual environment. It is recommended that all users determine the applicability of this information to their individual environments and take appropriate actions. All aspects of this Security Configuration Guide are subject to change without notice and on a case-by-case basis. Your use of the information contained in this document or materials linked herein is at your own risk. Dell reserves the right to change or update this document in its sole discretion and without notice at any time.

Scope of the document

This document covers the security features supported by Omnia 1.4.

Document references

In addition to this guide, more information on Omnia can be found through the below links:

- [Omnia: Read Me](#)
- [Omnia: Quick Installation Guide](#)

Reporting security vulnerabilities

Dell takes reports of potential security vulnerabilities in our products very seriously. If you discover a security vulnerability, you are encouraged to report it to Dell immediately.

For the latest instructions on how to report a security issue to Dell, see the [Dell Vulnerability Response Policy](#) on the Dell.com site.

Follow us online

Follow Dell Security on these sites:

- dell.com/security
- dell.com/support

To provide feedback on this solution, email us at support@dell.com.

Security Quick Reference

Topics:

- [Security profiles](#)

Security profiles

Omnia requires root privileges during installation because it provisions the operating system on bare metal servers.

Product and Subsystem Security

Topics:

- Security controls map
- Authentication
- Login security settings
- User and credential management
- Authentication to external systems
- Deployment model
- Network security
- Data security
- Auditing and logging

Security controls map

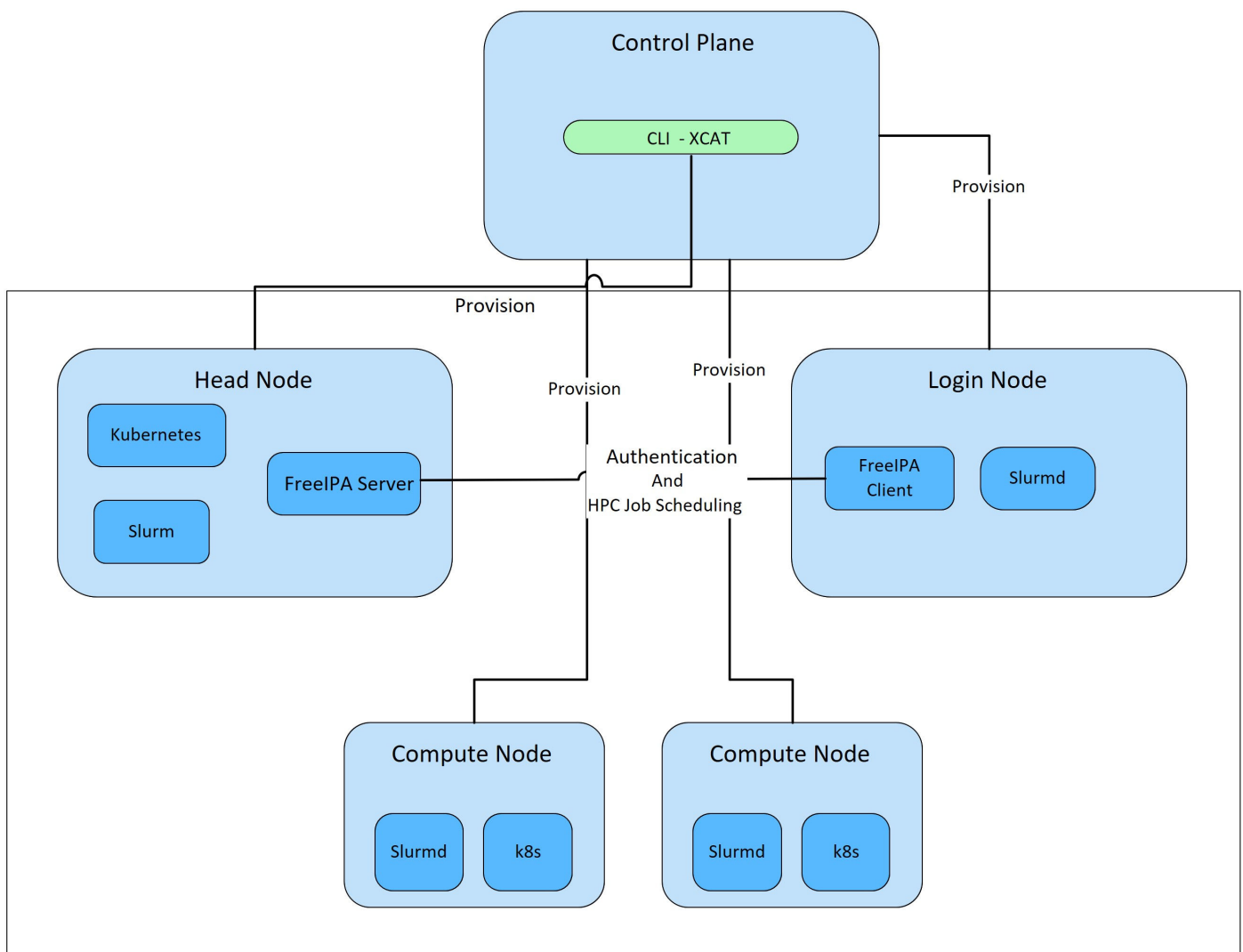


Figure 2. Cluster View

Omnia performs bare metal configuration to enable AI/HPC workloads. It uses Ansible playbooks to perform installations and configurations. iDRAC is supported for provisioning bare metal servers. Omnia installs xCAT to enable provisioning of clusters via PXE in different ways:

- Mapping file **[default]**: To dictate IP address/MAC mapping, a host mapping file can be provided.
- BMC discovery **[optional]**: To discover the cluster via BMC (iDRAC), IPMI must be enabled on remote servers. Discovery happens over IPMI. For security best practices when using this method, [click here](#).
- SNMP **[optional]**: To discover the cluster by querying switches, SNMPv2 must be enabled.
- Switch **[default]**: To discovery the cluster by routing communication through particular switch ports over SNMPv3, non-admin switch credentials must be provided.

i NOTE: IPMI is not required on the control plane. However compute nodes (iDRACs in the cluster/private network) require IPMI to be enabled for BMC discovery.

Omnia can be installed via CLI only. Slurm and Kubernetes are deployed and configured on the cluster. FreeIPA or LDAP is installed for providing authentication. To perform these configurations and installations, a secure SSH channel is established between the management node and the following entities:

- Manager Node
- Compute Nodes
- Login Node

Authentication

Omnia does not have its own authentication mechanism because bare metal installations and configurations take place using root privileges. Post the execution of Omnia, third-party tools are responsible for authentication to the respective tool.

Cluster authentication tool

In order to enable authentication to the cluster, Omnia installs FreeIPA: an open source tool providing integrated identity and authentication for Linux/UNIX networked environments. As part of the HPC cluster, the login node is responsible for configuring users and managing a limited number of administrative tasks. Access to the manager/head node is restricted to administrators with the root password. For authentication on the manager and compute nodes exclusively, LDAP can also be installed by Omnia on the client.

i NOTE: Omnia does not configure LDAP users or groups.

Authentication types and setup

Key-Based authentication

Use of SSH authorized_keys

A passwordless channel is created between the management station and compute nodes using SSH authorized keys. This is explained in [Security Controls Maps](#).

Login security settings

The following credentials have to be entered to enable different tools on the management station:

1. iDRAC (Username/ Password)
2. Ethernet Switch (Username/ Password)
3. Infiniband Switch (Username/ Password)
4. PowerVault ME4/ME5 (Username/ Password)
5. Provisioning OS (Password)

Similarly, passwords for the following tools have to be provided in `input/omnia_config.yml` to configure the cluster:

1. maria_db (Password)
2. DockerHub (Username/ Password)
3. FreeIPA (directory_manager_password, ipa_admin_password)

4. LDAP (ldap_bind_username, ldap_bind_password)

After the installation of Omnia is initialized, these files are validated and then encrypted using Ansible Vault and are hidden from external visibility and access.

User and credential management

Root user

The user calling Omnia should have root privileges during installation since Omnia involves bare metal installation and configuration.

Other users

After the installation of Omnia is complete, users can be created to run different workloads. After installation, Omnia need not be run again.

Authentication to external systems

Third party software installed by Omnia are responsible for supporting and maintaining manufactured-unique or installation-unique secrets.

Configuring remote connections

When setting up BeeGFS client services on the cluster, a connection authentication file is used to maintain the security of the communications between server and client.

1. Generate the connection authentication file (connAuth) and use it to set up BeeGFS meta, server and storage services.
2. Copy the connAuth file to the control plane and note the filepath.
3. Populate the value of `beegfs_secret_storage_filepath` in `input/storage_config.yml` with the filepath from the previous step.

Omnia will configure the BeeGFS clients on the cluster using the provided file. BeeGFS is responsible for maintaining and securing connAuthFile. For more information, [click here](#)

Deployment model

Omnia being open source, the product can be pulled from GitHub into the customer's environment. The customer should have a Linux server with CentOS version 8.3 and a stable network connection. Before deploying the Omnia control plane, ensure that the bare metal servers are connected to the PowerSwitches as per [the typical HPC layout](#). A single node Kubernetes cluster will be deployed on the management station. This K8s cluster will deploy and orchestrate the different containers of the control plane.

For more details regarding installation, see [Omnia: ReadMe](#).

Network security

Omnia configures the firewall as required by the third-party tools to enhance security by restricting inbound and outbound traffic to the TCP and UDP ports.

Network exposure

Omnia uses port 22 for SSH connections as Ansible uses port 22.

Firewall settings

Omnia configures the following ports for use by third-party tools installed by Omnia.

Table 1. Kubernetes ports requirements

Port Number	Layer 4 Protocol	Purpose	Type of Node
6443	TCP	Kubernetes API server	Manager
2379-2380	TCP	etcd server client API	Manager
10251	TCP	Kube-scheduler	Manager
10252	TCP	Kube-controller manager	Manager
10250	TCP	Kubelet API	Compute
30000-32767	TCP	Nodeport services	Compute
5473	TCP	Calico services	Manager/Compute
179	TCP	Calico services	Manager/Compute
4789	UDP	Calico services	Manager/Compute
8285	UDP	Flannel services	Manager/Compute
8472	UDP	Flannel services	Manager/Compute

Table 2. Slurm port requirements

Port Number	Layer 4 Protocol	Purpose	Type of Node
6817	TCP/UDP	Slurmd Port	Manager
6818	TCP/UDP	Slurmd Port	Compute
6819	TCP/UDP	Slurmd Port	Manager

Table 3. BeeGFS port requirements

Port Number	Layer 4 Protocol	Purpose	Tool
8008	TCP/UDP	Management service (beegfs-mgmt)	BeeGFS
8003	TCP/UDP	Storage service (beegfs-storage)	BeeGFS
8004	TCP/UDP	Client service (beegfs-client)	BeeGFS
8005	TCP/UDP	Metadata service (beegfs-meta)	BeeGFS
8006	TCP/UDP	Helper service (beegfs-helper)	BeeGFS

Table 4. xCAT port requirements

Port Number	Layer 4 Protocol	Purpose	Tool
3001	TCP/UDP	xcatsdport	xCAT
3002	TCP/UDP	xcatsiport	xCAT
3003	TCP	xcatslport	xCAT
7	UDP	echo	xCAT
22	TCP/UDP	SSH	xCAT
873	TCP/UDP	rsync	xCAT

Table 4. xCAT port requirements (continued)

Port Number	Layer 4 Protocol	Purpose	Tool
53	TCP/UDP	Domain	xCAT
67	TCP/UDP	bootps/DHCP	xCAT
68	TCP/UDP	DHCPC/bootpc	xCAT
69	TCP/UDP	TFTP	xCAT
80	TCP/UDP	WWW	xCAT
88	TCP/UDP	Kerberos	xCAT
111	UDP	Sunrpc	xCAT
443	TCP/UDP	HTTPS	xCAT
514	TCP/UDP	Shell, rsyslogd	xCAT
544	TCP	kshell	xCAT
657	TCP	RMC	xCAT
782	TCP	Conserver	xCAT
1058	TCP	nim	xCAT
2049	TCP/UDP	nfsd	xCAT
4011	TCP	PXE	xCAT
300	TCP	awk	xCAT
623	TCP/UDP	IPMI	xCAT
161	TCP/UDP	SNMP	xCAT
162	TCP/UDP	snmptrap	xCAT
5432	TCP	postgresDB	xCAT

Table 5. FreeIPA port requirements

Port Number	Layer 4 Protocol	Purpose	Type of Node
80	TCP	HTTP/HTTPS	Manager/ Login_Node
443	TCP	HTTP/HTTPS	Manager/ Login_Node
389	TCP	LDAP/LDAPS	Manager/ Login_Node
636	TCP	LDAP/LDAPS	Manager/ Login_Node
88	TCP/UDP	Kerberos	Manager/ Login_Node
464	TCP/UDP	Kerberos	Manager/ Login_Node
53	TCP/UDP	DNS	Manager/ Login_Node
7389	TCP	Dogtag's LDAP server	Manager/ Login_Node
123	UDP	NTP	Manager/ Login_Node

NOTE: To avoid security vulnerabilities, protocols can be restricted on the network using the parameters **restrict_program_support** and **restrict_softwares**. However, certain protocols are essential to Omnia's functioning and cannot be disabled: ftp, smbd, nmbd, automount, portmap. For more information on restricting network protocols, [click here](#).

Data security

Omnia does not store data. The passwords Omnia accepts as input to configure the third party tools are validated and then encrypted using Ansible Vault.

For more information on the passwords used by Omnia, see [Login Security Settings](#)

Auditing and logging


Omnia creates a log file at `/var/log/omnia.log` on the management station. The events during the installation of Omnia are captured as logs. There are separate logs generated by the third party tools installed by Omnia.

Logs

The logs are captured at `/var/log` in the file `omnia.log`. A sample is provided below:

```
2021-02-15 15:17:36,877 p=2778 u=omnia n=ansible | [WARNING]: provided hosts
list is empty, only localhost is available. Note that the implicit localhost does not
match 'all'
2021-02-15 15:17:37,396 p=2778 u=omnia n=ansible | PLAY [Executing omnia roles]
*****
2021-02-15 15:17:37,454 p=2778 u=omnia n=ansible | TASK [Gathering Facts]
*****
*
2021-02-15 15:17:38,856 p=2778 u=omnia n=ansible | ok: [localhost]
2021-02-15 15:17:38,885 p=2778 u=omnia n=ansible | TASK [common : Mount Path]
*****
2021-02-15 15:17:38,969 p=2778 u=omnia n=ansible | ok: [localhost]
```

These logs are intended to enable debugging.

 **NOTE:** The Omnia product recommends the product users to apply masking rules on personal identifiable information (PII) in the logs before sending to external monitoring application or source.

Logging format

Every log message begins with a timestamp and also carries information on the invoking play and task.

The format is described in the following table.

Field	Format	Sample Value
Timestamp	yyyy-mm-dd h:m:s	2021-02-15 15:17:37
Process Id	p=xxxx	p=2778
User	u=xxxx	u=omnia
Name of the process executing	n=xxxx	n=ansible
The task being executed/ invoked	PLAY/TASK	PLAY [Executing omnia roles] TASK [Gathering Facts]
Error	fatal: [hostname]: Error Message	fatal: [localhost]: FAILED! => {"msg": "lookup_plugin.lines"}
Warning	[WARNING]: warning message	[WARNING]: provided hosts list is empty

Miscellaneous Configuration and Management Elements

Topics:

- [Licensing](#)
- [Protect authenticity](#)
- [Ansible security](#)

Licensing

Omnia 1.4 is licensed under the Apache License 2.0.

A permissive license whose main conditions require preservation of copyright and license notices. Contributors provide an express grant of patent rights. Licensed works, modifications, and larger works may be distributed under different terms and without source code.

Protect authenticity

Every GitHub push requires a sign-off and a moderator is required to approve pull requests. All contributions have to be certified using the Developer Certificate of Origin (DCO)

```
Developer Certificate of Origin
Version 1.1
```

```
Copyright (C) 2004, 2006 The Linux Foundation and its contributors.
1 Letterman Drive
Suite D4700
San Francisco, CA, 94129
```

```
Everyone is permitted to copy and distribute verbatim copies of this
license document, but changing it is not allowed.
```

```
Developer's Certificate of Origin 1.1
```

```
By making a contribution to this project, I certify that:
```

- ```
(a) The contribution was created in whole or in part by me and I
 have the right to submit it under the open source license
 indicated in the file; or

(b) The contribution is based upon previous work that, to the best
 of my knowledge, is covered under an appropriate open source
 license and I have the right under that license to submit that
 work with modifications, whether created in whole or in part
 by me, under the same open source license (unless I am
 permitted to submit under a different license), as indicated
 in the file; or

(c) The contribution was provided directly to me by some other
 person who certified (a), (b) or (c) and I have not modified
 it.

(d) I understand and agree that this project and the contribution
 are public and that a record of the contribution (including all
 personal information I submit with it, including my sign-off) is
```

maintained indefinitely and may be redistributed consistent with this project or the open source license(s) involved.

## Ansible security

For the security guidelines of Ansible modules, go to [Developing Modules Best Practices: Module Security](#).

## Ansible vault

Ansible vault enables encryption of variables and files to protect sensitive content such as passwords or keys rather than leaving it visible as plaintext in playbooks or roles. Please refer [Ansible Vault guidelines](#) for more information.