HyTrust Appliance
Administration Guide

Version 3.0.2
October, 2012
## CONTENTS

List of Figures ........................................................................................................................................ 7

Preface .................................................................................................................................................. 11

CHAPTER 1  Getting Started ............................................................................................................15
  HTA Management Console ................................................................................................................... 15
  Starting the HTA Management Console .............................................................................................. 15
  Appliance Dashboard ............................................................................................................................. 17

CHAPTER 2  Using a Directory Service to Control Access to the Appliance .........................19
  HTA Authentication and Authorization Overview ............................................................................ 19
  Configuring Active Directory ............................................................................................................. 20
    Granting Privileges to a Service Account in Active Directory ......................................................... 21
    Creating Security Groups in Active Directory .............................................................................. 22

CHAPTER 3  Appliance Configuration ...........................................................................................25
  Configuring Network .............................................................................................................................. 25
    Network ............................................................................................................................................. 25
    Static Routes ..................................................................................................................................... 28
  Unified Authentication ........................................................................................................................... 29
    Prerequisites ..................................................................................................................................... 30
    Integrating the Appliance with Active Directory ............................................................................ 30
  Two-Factor Authentication ................................................................................................................... 35
    Prerequisites ..................................................................................................................................... 35
    RSA SecurID ..................................................................................................................................... 35
    CA AuthMinder ................................................................................................................................. 38
  Root Password Vaulting ..................................................................................................................... 39
    Prerequisites ..................................................................................................................................... 40
    Set Recovery Passcode ....................................................................................................................... 40
    Enable Root Password Vaulting ......................................................................................................... 41
    Request a Temporary Root Password .............................................................................................. 41
    Cancel a Temporary Root Password ............................................................................................... 43
  Managing Hosts ....................................................................................................................................... 44
    Adding Hosts to the HTA .................................................................................................................. 44
    Modifying HTA Protected Hosts ....................................................................................................... 45
    Removing HTA Protected Hosts ......................................................................................................... 45
    Configuring a Golden Host ................................................................................................................. 45
CHAPTER 4  Hardening Hypervisors ................................................................................. 63
  Host Compliance ........................................................................................................ 63
  Assessing ESX and ESXi Hosts ................................................................................ 64
  Remediating ESX and ESXi Hosts .......................................................................... 66
  Assessment History .................................................................................................... 67
    Summary .................................................................................................................. 67
    Hosts ....................................................................................................................... 67
    Details ...................................................................................................................... 69
    Templates ................................................................................................................ 69
  Host Configuration Templates ..................................................................................... 70
    Export Template ...................................................................................................... 70
    Import Template .................................................................................................... 71

CHAPTER 5  Creating and Deploying Access Policies ...................................................... 73
  Overview ................................................................................................................... 73
    Viewing the Current Policy ................................................................................... 75
    Changing the Current Policy ............................................................................... 75
  Policy Definitions and Behavior ............................................................................... 76
    Policy Resource ..................................................................................................... 76
    Roles ....................................................................................................................... 76
    Domain User Group ............................................................................................ 77
    Rules ...................................................................................................................... 77
    Constraints .......................................................................................................... 78
    RuleSets ................................................................................................................. 79
    Labels .................................................................................................................... 81
  Separation of Duties ............................................................................................... 82
  Policy Interaction ..................................................................................................... 83
  Example Policies ....................................................................................................... 83
    Example 1—Allow DevGroup to Create Virtual Machines on DevCluster Hosts ........ 83
    Example 2—Allow Two Different Administrator Groups to Use Separate Host Clusters and Inventory Folders .................................................................................. 84
    Example 3—Allow Two Different Administrator Groups to Manage Separate Virtual Machines Using OS Label ......................................................................................... 84
APPENDIX C  Root Password Recovery................................................................. 123
  Recovering From the HTA.............................................................................. 123
  Recovering From A Client System.............................................................. 124

APPENDIX D  Protecting ESX/ESXi Hypervisors ............................................. 125
  Mapped Mode ......................................................................................... 125
  Router Mode ......................................................................................... 125

APPENDIX E  Search Filters ............................................................................ 129

APPENDIX F  Cisco Nexus 1000V Software Switch Protection ...................... 131

APPENDIX G  HTA Command Line Interface .................................................. 133
  asc auth ............................................................................................ 134
  asc backup ....................................................................................... 134
  asc certs .......................................................................................... 136
  asc firewall ...................................................................................... 139
  asc ha ............................................................................................. 140
  asc log ............................................................................................. 142
  asc monitor ...................................................................................... 144
  asc network ..................................................................................... 145
  asc policy ....................................................................................... 148
  asc route ......................................................................................... 148
  asc service ...................................................................................... 150
  asc ssh ............................................................................................ 152
  asc upgrade ..................................................................................... 153
<p>| Figure 3-1 | HTA Management Console login screen ................................................................. 16 |
| Figure 3-2 | Appliance Dashboard page ...................................................................................... 17 |
| Figure 3-3 | Memory Usage ......................................................................................................... 18 |
| Figure 2-1 | Create HTA service account in AD ......................................................................... 21 |
| Figure 2-2 | New HTA service account in AD ............................................................................ 22 |
| Figure 2-3 | HTA AD security groups ........................................................................................ 23 |
| Figure 3-1 | Mapped Mode network configuration page .............................................................. 26 |
| Figure 3-2 | Router Mode network configuration page ............................................................... 27 |
| Figure 3-3 | Static Routes configuration page ............................................................................ 28 |
| Figure 3-4 | Add Static Routes page ........................................................................................ 28 |
| Figure 3-5 | HTA Authentication and Authorization process .................................................... 30 |
| Figure 3-6 | Authentication configuration page .......................................................................... 30 |
| Figure 3-7 | AD Conversion Wizard - Configure Service Account page ..................................... 31 |
| Figure 3-8 | AD Conversion Wizard - Active Directory Advanced Settings page ..................... 32 |
| Figure 3-9 | AD Conversion Wizard - Rule Conversion page ....................................................... 33 |
| Figure 3-10 | Configuration &gt; Authentication page in Directory Service mode ........................... 34 |
| Figure 3-11 | Configuration &gt; Two-Factor - RSA SecurID tab ..................................................... 36 |
| Figure 3-12 | RSA SecurID configuration file uploaded .............................................................. 36 |
| Figure 3-13 | HTA RSA SecurID login page ................................................................................ 37 |
| Figure 3-14 | Change RSA SecurID PIN page ............................................................................. 37 |
| Figure 3-15 | RSA SecurID PIN updated page ............................................................................ 37 |
| Figure 3-16 | Configuration &gt; Two-Factor - CA AuthMinder tab ................................................. 38 |
| Figure 3-17 | HTA CA Arcot login page ...................................................................................... 39 |
| Figure 3-18 | Root Password Vaulting configuration page ........................................................... 40 |
| Figure 3-19 | Host - General tab page ....................................................................................... 41 |
| Figure 3-20 | Compliance &gt; Hosts page .................................................................................... 42 |
| Figure 3-21 | Issue temporary password page .......................................................................... 42 |
| Figure 3-22 | Temporary password page ................................................................................... 42 |
| Figure 3-23 | HTA login credentials verification ....................................................................... 43 |
| Figure 3-24 | Cancelling a temporary password ....................................................................... 44 |
| Figure 3-25 | Compliance &gt; Hosts page ................................................................................... 44 |
| Figure 3-26 | Compliance &gt; Hosts &gt; Edit Host page - Advanced tab .......................................... 45 |
| Figure 3-27 | Enable Misc.enableTBoot setting ........................................................................ 47 |
| Figure 3-28 | Configuration &gt; Trusted Execution page ............................................................. 47 |
| Figure 3-29 | Enter known TPM digest value ............................................................................ 48 |
| Figure 3-30 | Selecting Intel TXT ESXi hosts ............................................................................ 48 |
| Figure 3-31 | Trusted ESXi hosts .............................................................................................. 48 |
| Figure 3-32 | Trusted policy labels .......................................................................................... 49 |
| Figure 3-33 | Scheduled Events page ....................................................................................... 49 |
| Figure 3-34 | Add Scheduled Event page .................................................................................. 50 |
| Figure 3-35 | Add Host to Scheduled Event page ...................................................................... 51 |
| Figure 3-36 | Edit Scheduled Event page .................................................................................. 51 |
| Figure 3-37 | Configure SMTP notifications and SNMP monitoring ......................................... 53 |</p>
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3-38</td>
<td>Configuration &gt; Certificates page</td>
<td>54</td>
</tr>
<tr>
<td>3-39</td>
<td>Certificate details page</td>
<td>54</td>
</tr>
<tr>
<td>3-40</td>
<td>Generate Certificates page</td>
<td>54</td>
</tr>
<tr>
<td>3-41</td>
<td>Certificate CSR Data page</td>
<td>55</td>
</tr>
<tr>
<td>3-42</td>
<td>Certificate details page</td>
<td>55</td>
</tr>
<tr>
<td>3-43</td>
<td>Install Signed Certificate page</td>
<td>56</td>
</tr>
<tr>
<td>3-44</td>
<td>Configuration &gt; Certificates &gt; Certificate Authorities tab</td>
<td>57</td>
</tr>
<tr>
<td>3-45</td>
<td>Install Third-party Root Certificate page</td>
<td>57</td>
</tr>
<tr>
<td>3-46</td>
<td>Password Requirements configuration page</td>
<td>58</td>
</tr>
<tr>
<td>3-47</td>
<td>Configuration &gt; vCenter Plugin page</td>
<td>59</td>
</tr>
<tr>
<td>3-48</td>
<td>HyTrust tab in vSphere Client window</td>
<td>60</td>
</tr>
<tr>
<td>3-49</td>
<td>Configuration &gt; vCenter Plugin page</td>
<td>61</td>
</tr>
<tr>
<td>4-1</td>
<td>Compliance Hosts page</td>
<td>63</td>
</tr>
<tr>
<td>4-2</td>
<td>Test Results page</td>
<td>65</td>
</tr>
<tr>
<td>4-3</td>
<td>Compliance History - Summary tab</td>
<td>67</td>
</tr>
<tr>
<td>4-4</td>
<td>Compliance History - Hosts tab</td>
<td>67</td>
</tr>
<tr>
<td>4-5</td>
<td>Compliance Host Detail page</td>
<td>68</td>
</tr>
<tr>
<td>4-6</td>
<td>Compliance Test Results page</td>
<td>68</td>
</tr>
<tr>
<td>4-7</td>
<td>Compliance History - Details tab</td>
<td>69</td>
</tr>
<tr>
<td>4-8</td>
<td>Compliance History - Templates tab</td>
<td>69</td>
</tr>
<tr>
<td>4-9</td>
<td>HTA Templates page</td>
<td>70</td>
</tr>
<tr>
<td>4-10</td>
<td>Export / Import Templates page</td>
<td>71</td>
</tr>
<tr>
<td>5-1</td>
<td>Policy &gt; History page</td>
<td>74</td>
</tr>
<tr>
<td>5-2</td>
<td>Deployed Policy Resources page</td>
<td>75</td>
</tr>
<tr>
<td>5-3</td>
<td>Policy &gt; Resources page</td>
<td>76</td>
</tr>
<tr>
<td>5-4</td>
<td>Policy &gt; Roles page</td>
<td>77</td>
</tr>
<tr>
<td>5-5</td>
<td>Policy &gt; Rules page</td>
<td>78</td>
</tr>
<tr>
<td>5-6</td>
<td>Policy &gt; RuleSets page</td>
<td>79</td>
</tr>
<tr>
<td>5-7</td>
<td>Assign RuleSets page</td>
<td>80</td>
</tr>
<tr>
<td>5-8</td>
<td>RuleSet details page</td>
<td>81</td>
</tr>
<tr>
<td>5-9</td>
<td>Policy &gt; Labels page</td>
<td>81</td>
</tr>
<tr>
<td>5-10</td>
<td>Edit Role page</td>
<td>82</td>
</tr>
<tr>
<td>6-1</td>
<td>Configuration &gt; Secondary Approval page</td>
<td>88</td>
</tr>
<tr>
<td>6-2</td>
<td>Secondary Approval Wizard - Select Requestor Groups page</td>
<td>89</td>
</tr>
<tr>
<td>6-3</td>
<td>Secondary Approval Wizard - Select Resources page</td>
<td>89</td>
</tr>
<tr>
<td>6-4</td>
<td>Secondary Approval Wizard - Select vSphere Operations page</td>
<td>90</td>
</tr>
<tr>
<td>6-5</td>
<td>Secondary Approval Wizard - Select Approver Groups page</td>
<td>90</td>
</tr>
<tr>
<td>6-6</td>
<td>Secondary Approval Wizard - Control Summary page</td>
<td>91</td>
</tr>
<tr>
<td>6-7</td>
<td>Secondary Approval Controls tab</td>
<td>91</td>
</tr>
<tr>
<td>6-8</td>
<td>Policy &gt; Secondary Approval Requests page</td>
<td>91</td>
</tr>
<tr>
<td>6-9</td>
<td>Secondary Approval Pending Request page</td>
<td>92</td>
</tr>
<tr>
<td>6-10</td>
<td>Secondary Approval Pending Request - Approve page</td>
<td>93</td>
</tr>
<tr>
<td>6-11</td>
<td>Secondary Approval Pending Request page</td>
<td>94</td>
</tr>
<tr>
<td>6-12</td>
<td>Secondary Approval Pending Request - Deny page</td>
<td>94</td>
</tr>
<tr>
<td>6-13</td>
<td>Policy &gt; Secondary Approval Requests - History tab</td>
<td>95</td>
</tr>
<tr>
<td>6-14</td>
<td>Secondary Approval Request Details page</td>
<td>95</td>
</tr>
<tr>
<td>7-1</td>
<td>Configuration &gt; Logging page</td>
<td>100</td>
</tr>
<tr>
<td>7-2</td>
<td>General &gt; Log Viewer page</td>
<td>101</td>
</tr>
<tr>
<td>7-3</td>
<td>Message Detail</td>
<td>102</td>
</tr>
<tr>
<td>7-4</td>
<td>Configuration &gt; Logging page</td>
<td>104</td>
</tr>
<tr>
<td>8-1</td>
<td>HTA Dashboard with NRM and PHM status</td>
<td>106</td>
</tr>
<tr>
<td>8-2</td>
<td>HTA CLI with NRM and PHM status</td>
<td>107</td>
</tr>
<tr>
<td>9-1</td>
<td>Maintenance &gt; License page</td>
<td>109</td>
</tr>
<tr>
<td>9-2</td>
<td>Maintenance &gt; License - Upgrade tab</td>
<td>110</td>
</tr>
<tr>
<td>Figure 9-3</td>
<td>Maintenance &gt; Services page</td>
<td>110</td>
</tr>
<tr>
<td>Figure 9-4</td>
<td>Maintenance &gt; Troubleshooting page</td>
<td>111</td>
</tr>
<tr>
<td>Figure 9-5</td>
<td>Maintenance &gt; Jobs page</td>
<td>112</td>
</tr>
<tr>
<td>Figure 9-6</td>
<td>General &gt; Search page</td>
<td>113</td>
</tr>
<tr>
<td>Figure 9-7</td>
<td>General &gt; Search page resource tree path</td>
<td>113</td>
</tr>
<tr>
<td>Figure D-1</td>
<td>Sample HTA host vSwitch</td>
<td>126</td>
</tr>
<tr>
<td>Figure D-2</td>
<td>HTA host in Router Mode</td>
<td>127</td>
</tr>
<tr>
<td>Figure F-1</td>
<td>Policy &gt; Roles page</td>
<td>132</td>
</tr>
</tbody>
</table>
List of Figures
The HyTrust Appliance (HTA) provides a centralized point of control for hypervisor configuration, compliance, and access management.

This guide assumes you have already deployed the HyTrust Appliance (HTA) as a virtual machine on a VMware ESX (4.0/4.1) or ESXi (4.0/4.1/5.0) host. If not, refer to the *HyTrust Appliance Installation Guide* for details.

This document describes how to administer the HTA using the HTA Management Console and other applicable tools.

This guide does not discuss installation of the HTA. See the *HyTrust Appliance Installation Guide* for more information.

**Audience**

This guide is intended for information technology personnel who are reasonably proficient in the following areas:

- Using VMware vSphere
- Networking and route configuration
- Microsoft Active Directory (AD)
- Policy Management

**Document Organization**

This guide is organized into the following sections:

- **Chapter 1, Getting Started**—Provides information on the HTA Management Console.
- **Chapter 2, Using a Directory Service to Control Access to the Appliance**—Describes how to configure a directory service to authenticate and authorize HTA and vSphere users.
- **Chapter 3, Appliance Configuration**—Describes the various configuration options available in the HTA Management Console.
- **Chapter 4, Hardening Hypervisors**—Provides details on how to manage host compliance.
- **Chapter 5, Creating and Deploying Access Policies**—Describes how to manage HTA access policies.
- **Chapter 6, Secondary Approval**—Describes how to setup and configure the HTA to require approval for disruptive virtual machine operations.
- **Chapter 7, Logging**—Describes how to setup and configure the HTA for logging, and collect the HTA troubleshooting log bundle.
Preface

- **Chapter 8, Monitoring Hosts and Networks**—Describes the various monitoring features available on the HTA.
- **Chapter 9, Maintaining the Appliance**—Provides information on managing HTA licenses, services, logs, jobs, and performing searches.
- **Appendix A, Default Appliance Roles and Permissions**—Provides details about the roles and permissions associated with the default HTA user groups.
- **Appendix B, Summary of All HTA Management Console Operations**—Provides a list of all HTA Management Console menu items.
- **Appendix C, Root Password Recovery**—Describes how to perform an emergency recovery of the root user password on a host.
- **Appendix D, Protecting ESX/ESXi Hypervisors**—Provides information on some additional requirements needed to protect HTA hosts.
- **Appendix E, Search Filters**—Provides information on using search filters for searching HTA resources.
- **Appendix F, Cisco Nexus 1000V Software Switch Protection**—Describes the HTA features for controlling Cisco Nexus 1000V operations.
- **Appendix G, HTA Command Line Interface**—Describes and provides examples of all HTA command line interface (CLI) commands.

**Document Conventions**

The table below summarizes the call-outs and icons used in this guide.

**Call-outs and Icons**

<table>
<thead>
<tr>
<th>Call-out or Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note:</td>
<td>Indicates supporting information to the document text.</td>
</tr>
<tr>
<td><strong>IMPORTANT:</strong></td>
<td>Provides important information that should be highly considered.</td>
</tr>
</tbody>
</table>

The table below summarizes the typographical conventions used in this guide.

**Typographical conventions**

<table>
<thead>
<tr>
<th>Style</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold</strong></td>
<td>Menu items.</td>
</tr>
<tr>
<td><em>Italic</em></td>
<td>Provides emphasis and identifies user interface items and document titles.</td>
</tr>
<tr>
<td><strong>Monospace</strong></td>
<td>Command names, console text, and file names.</td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td>Contains information for which you must supply a value.</td>
</tr>
<tr>
<td></td>
<td>Separates a set of choices from which only one may be chosen.</td>
</tr>
<tr>
<td>{ }</td>
<td>Required command parameters that must be specified.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Optional command parameters.</td>
</tr>
</tbody>
</table>

**Related References**

For more information about the HTA refer to the following resources:
Contacting HyTrust

If you require additional information or technical support, contact us at:

Phone: (650) 681-8100
Email: info@hytrust.com
Website: http://www.hytrust.com
Preface
Getting Started

This chapter contains the following sections:
- HTA Management Console
- Appliance Dashboard

HTA Management Console

You use the web-based HTA Management Console to customize HTA configuration settings and set up policies for safeguarding your managed virtual infrastructure environment. For example, the management console provides menus to set authentication options for users, add vCenter Server and hosts to the protected infrastructure, define templates and policy checks/tests to enforce security of protected virtual infrastructure, and view and configure logs.

Refer to Appendix B. Summary of All HTA Management Console Operations for a list of all HTA Management Console menu items.

Starting the HTA Management Console

After you complete the initial configuration, as discussed in the HyTrust Appliance Installation Guide, any authorized user can now access the web-based HTA Management Console to set up the HTA to safeguard your managed virtual infrastructure environment.

To start the HTA Management Console:

1. Open a web browser and enter the URL location of the HTA virtual machine (as shown in the vSphere Client console after powering up the HTA virtual machine). For example: https://hta.example.com/asc

Note: Only secure HTTPS sessions are supported; HTTP connections are blocked.
2. The login screen appears.

![HyTrust Login Screen](image)

*Figure 1-1    HTA Management Console login screen*

3. Enter your HTA username and password, and click Login.

*Note:* If you are still running in Demo mode, use the username (*superadminuser*) and password (*Pa$$w0rd123!* to log into the system.

If you are using Active Directory (AD) authentication and roles, you can log in using an HTA user who is a member of the default *HT_SuperAdmin* group. See Appendix A, *Default Appliance Roles and Permissions* for a list of available HTA roles and the corresponding permissions granted to group members on login.
Appliance Dashboard

The Appliance Dashboard appears after you successfully log into the HTA Management Console, or select **General > Appliance Dashboard** from the menu.

**Figure 1-2 Appliance Dashboard page**

The Dashboard displays a summary of the following HTA information:

- **General**—Includes the hostname, appliance ID, installed software version, network deployment type, and the management IP address.
- **License Information**—Includes the customer name, entitlement number, status, maximum number of protected hosts allowed, type, and maintenance and support expiration dates.
- **Services**—Shows the status of all HTA related services.
- **Resources**—Includes the state and usage of various HTA related resources (e.g., CPU, disk, and memory usage; certificate and network status). HTA administrators can monitor system usage and take appropriate actions as needed (e.g., Disk is 80% full).

You can click the green bars representing CPU, disk, or memory usage percent to view detailed graphs that show usage by day, week, month, and year.
For example, the following figure shows memory usage:

**Figure 1-3 Memory Usage**

Refer to Chapter 8, Monitoring Hosts and Networks for more information on monitoring HTA-protected hosts and networks.

- **Compliance**—Shows the overall percentage of host conformance with the current compliance configuration in the HTA-protected environment.
- **Protection**—Shows the overall percentage of hosts protected in the HTA-protected environment.
Using a Directory Service to Control Access to the Appliance

This chapter contains the following sections:

- HTA Authentication and Authorization Overview
- Configuring Active Directory

HTA Authentication and Authorization Overview

The HTA operates using the following user authentication modes:

- Demo (only supports default, built-in users)
- Directory Service—Microsoft® Active Directory (AD). In addition, the HTA can be configured with RSA SecurID or CA Arcot—see Two-Factor Authentication on page 35.

By default, the HTA operates in Demo mode after installation and remains that way until the HTA configuration is changed to use Directory Service mode authentication.

Note: Demo mode is only intended for product evaluation and testing, not production environments. Once you install the HTA in a production environment and complete the initial configuration, it is recommended that you immediately convert the HTA to use Directory Service mode.

While in Demo mode the HTA contains a number of uniquely defined roles. There are several special demo users (stored locally) who are assigned specific roles to access and perform operations on the virtual infrastructure. Demo users cannot be modified and you cannot change their passwords. The default password for all Demo users is Pa$$w0rd123!. The roles available in Demo mode are listed in Appendix A, Default Appliance Roles and Permissions.
Once the HTA is configured for Directory Service mode authentication and authorization, Demo mode cannot be re-enabled.

While converting the HTA to Directory Service mode, default rules are created that map existing user groups in the directory service to the default HTA roles. This allows administrators to enable role-based access to the virtual infrastructure simply by adding the user identities to these directory groups, based on their individual responsibilities. Refer to Appendix A, Default Appliance Roles and Permissions for a description of each role.

Instead of using the existing directory service security groups, you may find it helpful to manually create specific groups in your directory service for each HTA group prior to converting the HTA to Directory Service mode. This would allow for a 1:1 mapping between directory group names and HTA roles. At a minimum, one directory security group (e.g., HT_SuperAdmin) must be mapped to the ASC_SuperAdmin role in the HTA.

Administrators can define custom rules that restrict entitlement based on the specific virtual infrastructure objects their users need to access and manage. Rules that define entitlement can be based on the pre-defined roles described in Appendix A, Default Appliance Roles and Permissions, or administrators can use custom user-defined roles.

Rules can be thought of as a relationship between a group, one or more objects, and one HTA role. The directory group has a defined entitlement based on a rule. The entitlement specifies operations that users in the group may perform on the objects.

For example, the ASC_NetworkAdmin role specifies, among other things, privileges to perform AddPortGroup and RemoveVirtualSwitch operations. Therefore, all members of the HT_NetworkAdmin directory security group are allowed to perform these operations on a policy resource, such as an HTA managed vCenter Server, and all objects, including the networking subsystem, in that vCenter Server.

A collection of rules currently enforced by the HTA constitutes an active or deployed policy. Policy, rules, and role definitions can be defined using the HTA Management Console. Further details regarding policy, rules, and roles can be found in Chapter 5, Creating and Deploying Access Policies.

### Configuring Active Directory

To use Active Directory (AD) for authenticating virtual infrastructure users as well as HTA Management Console users, the HTA must be in Directory Service mode. Before you can make the switch from Demo mode to Directory Service mode you need to create an HTA service account in your AD server.

Prior to creating the HTA service account, ensure you have a good understanding of where the service accounts, groups, and users are currently stored in AD. The HTA supports the ability to have the service account in one container (cn) or organizational unit (ou) while the HTA groups reside in a different cn or ou. Support for multiple domains within a single AD forest is also available by utilizing the advanced settings within the AD conversion wizard. For further explanation of Advanced AD mode, see Integrating the Appliance with Active Directory on page 30.

The HTA integrates directly with AD via LDAP protocols using the HTA service account credentials. The HTA uses the service account to query AD and ascertain the appropriate group membership for the users. This interaction occurs each time a user attempts to access the virtual infrastructure.
The following sections provide step-by-step instructions on how to create an HTA service account in AD and grant privileges to it, as well as how to create HTA security groups in AD.

Granting Privileges to a Service Account in Active Directory

Perform the following to create a new service account in AD:

1. Login to the Windows host machine running your AD server using credentials that have sufficient privileges to create new accounts.
2. In AD, add a new user to serve as the HTA service account (e.g., HtaServiceAccount).

   **Note:** You must create a unique service account. Do not use a built-in Administrator account as a service account. The service account may be located in any container or organizational unit. In this example, HtaServiceAccount is in the service ou, users are in two separate ous (employees and non-employees), and HTA groups are in the securitygroups ou.

3. Click Next.
4. When you are asked to assign the password to the new service account:
   a. Enter the password in the Password and Confirm password fields.
   b. Deselect the User must change password at next logon checkbox.
   c. Select the Password never expires checkbox.

   ![Create HTA service account in AD](image.png)
5. Click Next.

![Figure 2-2 New HTA service account in AD]

After the new HTA service account is created it only has query privileges on the HTA server AD forest. In some environments, the AD administrator may have modified the default account privileges.

The HTA service account requires the following permissions in AD:

- Domain object: Read memberOf
- User object: attributes memberOf and distinguishedName
- Group object: attributes member, memberOf, and distinguishedName

If needed, work with your AD administrator to configure these permissions for the HTA service account.

**Creating Security Groups in Active Directory**

As previously noted, default HTA rules are created by mapping existing user groups in AD to default roles in the HTA when the HTA is converted to Directory Service mode. In a complex environment with a large number of administrators, it is common to create unique AD group names that correspond to each of the HTA default roles. At a minimum, one AD security group (e.g., HT_SuperAdmin) must be mapped to the ASC_SuperAdmin role in the HTA in order for AD conversion to be successful. AD group names do not need to follow the HTA naming convention.

Perform the following to create the HTA security groups in AD:

1. Create a security group for each HTA role described in Appendix A, Default Appliance Roles and Permissions.
2. For each group, assign the Group scope to *Global* and the Group type to *Security*. 
Note: The HTA supports security groups with domain local, domain global, and/or universal scope. Check with your AD administrator to confirm the proper setting for your environment.

In the figure below, the HTA groups are located in the securitygroups ou.

![Figure 2-3 HTA AD security groups](image)

After you setup the HTA service account and decide which security groups in AD to use, you may switch over at any time to use AD for user authentication. However you will not be allowed to switch back to the Demo mode. Follow the steps in Integrating the Appliance with Active Directory on page 30 to convert the HTA to Directory Service mode.
Using a Directory Service to Control Access to the Appliance

Configuring Active Directory
Appliance Configuration

This chapter contains the following sections:

- Configuring Network
- Unified Authentication
- Two-Factor Authentication
- Root Password Vaulting
- Managing Hosts
- Scheduling Events
- Retrieving vCenter Server Events
- Configuring Notifications
- Managing Certificates
- Changing Password Requirements for ascadminuser
- Third Party Configuration
- vCenter Server Plugin

Configuring Network

This section contains information on configuring the HTA network mode (Mapped Mode or Router Mode) and static routes.

Network

The Network Configuration page (Configuration > Network) displays the current network settings for the HTA. The information displayed depends on whether you are using Mapped Mode or Router Mode for your network deployment.
Mapped Mode

The following page appears in Mapped Mode.

Figure 3-1 Mapped Mode network configuration page

Use the Appliance Identity and Management Interface section to configure the HTA network interface. The following fields are available:

- Fully Qualified Hostname—The fully qualified domain name (FQDN) of the HTA (e.g., hta.example.com).
- Connection 1: IP Address—The IP address of the HTA on the network.
- Connection 1: Mask—The subnet mask of the HTA on the network.
- Gateway—The IP address of the gateway the HTA uses.
- List of DNS Server IP Addresses—A comma-separated list of DNS servers for the HTA to use (e.g., 172.16.2.20, 10.10.1.4).

Note: The DNS Server information was initially specified during the initial setup and configuration of the HTA when it was installed.

Use the NTP Servers section to configure the network time servers for the HTA. The following fields are available:

- Enable NTP Servers—Enables (selected) or disables (deselected) using a network time server with the HTA. The default is deselected.
- NTP Servers—A comma-separated list of NTP server IP addresses for the HTA to use.
Router Mode

The following page appears in Router Mode.

Use the Router Interface section to configure the HTA network interface. The following fields are available:

- Enable Routing Information Protocol Service—Enables (selected) or disables (deselected) using the Routing Information Protocol (RIP), a widely deployed interior gateway protocol. Select this checkbox if you are deploying in a network where RIP is currently enabled. The HTA supports both RIPv1 and RIPv2. The default is deselected.
- Router Password—The remote configuration password for RIPv2 services.
- Fully Qualified Hostname—The fully qualified domain name (FQDN) of the HTA (e.g., hta.example.com).
- Connection 1: IP Address—The IP address of the HTA management interface (eth0) on the public network.
- Connection 1: Mask—The subnet mask of the HTA management interface (eth0) on the public network.
- Connection 2: IP Address—The IP address of the HTA interface (eth1) on the protected network.
- Connection 2: Mask—The subnet mask of the HTA interface (eth1) on the protected network.
- Gateway—The IP address of the gateway the HTA uses.
- List of DNS Server IP Addresses—A comma-separated list of DNS servers for the HTA to use (e.g., 172.16.2.20, 10.10.1.4).
Appliance Configuration
Configuring Network

**Note:** The DNS Server information was initially specified during the initial setup and configuration of the HTA when it was installed.

Use the *NTP Servers* section to configure the network time servers for the HTA. The following fields are available:

- Enable NTP Servers—Enables (selected) or disables (deselected) using a network time server with the HTA.
- NTP Servers—A comma-separated list of NTP server IP addresses for the HTA to use.

**Static Routes**

You may need to set a static route to the HTA if you are trying to access the HTA Management Console from a client that is not on the same subnet as the HTA.

The Static Routes page (**Configuration > Static Routes**) allows you to view any existing static routes and add new static routes.

![Static Routes configuration page](image)

Click the Add button to add a new static route. The Add Static Route page appears:

![Add Static Routes page](image)

The following settings are available:

- Network Address—The IP address of the client.
- Mask—The subnet mask of the client.
- Gateway—The gateway IP address where the client is located.
- Device—The interface to route the traffic through. Choices are:
  - Network 1—Route traffic through the eth0 interface.
  - Network 2—Route traffic through the eth1 interface.
  - Network 3—Route traffic through the eth2 interface.
In both Mapped Mode and Router Mode network configurations, select the Network 1 option for device type.

**Unified Authentication**

The HTA intercepts all requests destined for HTA-protected hosts (e.g., ESX, vCenter Server, Cisco UCS, Nexus 1000V) and authenticates the user against the Directory Service. Authentication of the user (including session ID) lasts for the full session. Once a session is established, authorization to perform a particular operation, including directory group membership, can occur on multiple occasions per session.

After the HTA authenticates the user it performs an authorization check for each request based on the local policy data. If authorized, the HTA forwards the request (using a special service account) to the target server.

The HTA has the ability to follow the domain controller and global catalog referrals in a single Active Directory forest. If your Active Directory environment is setup to follow referrals, please contact HyTrust Support to help you enable this feature in your HTA.

Here is an example of the authentication and authorization process using the vSphere Client:

1. The HTA obtains the user's identity when the user attempts to log in.
2. The HTA queries the Directory Service to authenticate the user and validate the user's password. The HTA also obtains information about the user's group membership to authorize every operation the user attempts to perform, for example:
   a. Identify the requested operation (i.e., start a virtual machine).
   b. Identify the object a user is targeting for an operation (i.e., VM mref 449).
   c. Query the HTA policy database to identify the list of user groups authorized to perform the requested operation on the specified object and determine if the current user is a member of an authorized user group.
   d. The HTA logs information about the operation, the user, and the object involved.

   If the user is authorized, the HTA reissues the operation request and sends it to the vCenter Server or ESX host to which the original login request was routed. Otherwise, the HTA returns an error message to the user.

   If the HTA cannot authenticate a user, the authentication fails and the user is denied access to the specified target. See Figure 3-5 for a diagram of this process.

Similarly, the HTA performs the following sequence when a user logs into an ESX host using an SSH client:

1. Identify the requested operation (i.e., change the iSCSI configuration on the server).
2. Identify the host a user is targeting for an operation (e.g.: esx54.example.com).
3. Query the HTA policy database to identify the list of user groups authorized to perform the requested operation on the specified object and determine if the current user is a member of an authorized user group.
4. The HTA logs information about the operation, the user, and the object involved.
If the user is authorized, the HTA reissues the operation request and sends it to the HTA protected host (e.g., vCenter Server, ESX) to which the original login request was routed. Otherwise, the HTA returns an error message to the user.

1. User attempts to login or perform an operation on a protected host.
2. HTA queries the directory service to authenticate user.
3. If user is authenticated, the HTA obtains the user’s group information for authorization of operations.
4. If user is authorized to perform the requested operation, the HTA sends the request to the protected host.
5. User receives success or error message.

Figure 3-5 HTA Authentication and Authorization process

An HTTP client goes through a similar authentication and authorization process.

Prerequisites

Before you configure the HTA to use a Directory Service (e.g., Active Directory) you must add an HTA service account and grant it the proper privileges (e.g., to create new accounts)—see Chapter 2, Using a Directory Service to Control Access to the Appliance.

Integrating the Appliance with Active Directory

IMPORTANT: Converting the HTA to Directory Service mode for authentication and authorization is non-reversible and Demo mode cannot be re-enabled.

To convert the HTA to Directory Service mode:

1. Open the Authentication Configuration page (Configuration > Authentication).

![Authentication Configuration page](image)

Figure 3-6 Authentication configuration page

2. Select the Directory Service radio button and click the Apply button.

The Active Directory Conversion Wizard opens, which guides you through the steps to connect the HTA to your directory service.
3. Fill in the following in the Root Domain section:
   - Root Domain Name—The root domain where your AD is located. Use the following format:
     - corp.example.com
     The HTA supports either a single or multiple domain forest. If your AD forest includes only a single domain, the forest root domain will include all your users, groups, and resources.

4. Use the Service Account section to specify the AD HTA service account information. The following fields are available:
   - SSL Enabled—Select this checkbox if your AD uses SSL. Deselect if your AD does not use SSL. SSL is disabled by default.
   - Service Account Name—The HTA service account user name in AD (e.g., htaserviceaccount).
     - If the service account is located in a different domain from the Root Domain, enter htaserviceaccount@subdomain.corp.example.com in this field.
   - Service Account Password—The AD password for your service account.
   - Confirm Service Account Password—Retype the AD password for your service account.

   **Note:** The HTA service account must exist in AD prior to converting the HTA to Directory Service mode.

   In most cases, this information should be sufficient to complete the conversion. The HTA uses the service account credentials to automatically discover the list of forest
Appliance Configuration
Unified Authentication

global catalogs and domain controllers to use when authenticating users. If the automatic discovery fails you will need to manually configure your AD information in the HTA by selecting the Proceed to Active Directory Advanced Settings checkbox.

5. Select the Proceed to Active Directory Advanced Settings checkbox in the Proceed to Advanced Settings section to:
   - Manually configure the preferred global catalog
   - Map domain controllers to domain names
   - Set custom ports
   - Enable SSL

6. Click Next.

7. If you selected the Proceed to Active Directory Advanced Settings checkbox the Active Directory Advanced Settings page appears.

![AD Conversion Wizard - Active Directory Advanced Settings page](image)

In most cases, the HTA should be able to auto detect all the domain controllers and global catalogs within your environment. However, if manual configuration is required use the following settings to configure your AD settings:

Root Domain section:
- Default Domain—Select the default domain for your AD from the drop down list.
Configuration Types section:
- Configuration Type—Select the Manual Configuration radio button to enable you to make changes to the fields on this page.
- Discovery Service Refreshing—The refresh interval for the discovery service.

Global Catalogs section:
- Preferred Global Catalog—Select your preferred global catalog from the drop down list.
- SSL Enabled—Select this checkbox if your global catalog uses SSL.
- Port—The global catalog port.

Domain Controllers section:
- SSL Enabled—Select this checkbox if your domain controllers use SSL.
- Port—The domain controllers port.

Note: The Add and Delete buttons in the Domain Controllers mapping section are only active when the Configuration Type is set to Manual Configuration.

When you are finished manually configuring the AD settings click Next.

8. The Rule Conversion page appears where you can map HTA roles to AD groups.

![Active Directory Conversion Wizard Rule Conversion](image)

Figure 3-9 AD Conversion Wizard - Rule Conversion page

In the HTA, rules are defined by their domain user group and assigned role. After this step, all the default HTA rules will be converted and mapped to AD groups.
Although not a requirement, it is recommended that you manually create HTA specific security groups in AD prior to conversion—see Creating Security Groups in Active Directory on page 22.

The following information and settings are available:

- Role—The HTA role name.
- Description—The description for the role.
- Domain Name—The AD domain name. Select the desired domain from the drop down list.
- Group Name—The AD security group name. Enter the AD group name you wish to associate with the default role. This field uses auto-fill to complete field entry. The name used in this field must be identical to the name found in AD.

**Note:** At a minimum, one AD security group (e.g., HT_SuperAdmin) must be mapped to the HTA ASC_SuperAdmin role in order for AD conversion to be successful.

9. Click Next.
10. A summary page appears confirming the AD settings. Review the information to make sure the Domain Controllers, Rule Conversion, and Service Account settings are accurate.
11. Click Finish to convert the HTA to Directory Service mode.

Once the conversion process is complete, you need to use your AD credentials to login to the HTA Management Console.

**Note:** Before you login to the HTA with your AD credentials, confirm that you have manually added users to the proper HTA security groups in AD. See Appendix A, Default Appliance Roles and Permissions for a list of available HTA roles, groups, and the corresponding permissions granted to group members when they login.

### Rerunning the Active Directory Conversion Wizard

If your AD properties change after converting the HTA to Directory Service mode you must rerun the Active Directory Conversion Wizard.

Perform the following to rerun the Active Directory Conversion Wizard:

1. Open the **Configuration > Authentication** page.

![Configuration > Authentication page in Directory Service mode](image)

2. Click the Update button.

   The **Active Directory Conversion Wizard** starts where you can make your necessary changes.
Two-Factor Authentication

HTA two-factor authentication requires the user to provide two forms of identification (a password/PIN and a token) to login.

The HTA supports the following two-factor authentication types:

- **RSA SecurID** (RSA AM-7.1.4-build20110516110107 with patch AM-7.1 SP4 and earlier)
- **CA AuthMinder** (WebFort version 6.2)

Prerequisites

- Two-factor authentication requires the HTA to be in Directory Service mode.
- The RSA SecurID server or CA AuthMinder server must be accessible to the HTA.

RSA SecurID

Configuring the HTA to use RSA SecurID authentication consists of the following tasks:

1. **Agent Host Configuration**
2. **Generating an RSA Configuration File**
3. **Configuring the Appliance for RSA SecurID**
4. **Creating a New PIN**

Agent Host Configuration

To facilitate communication between the HTA and the RSA Authentication Manager/RSA SecurID Appliance an Authentication Agent record must be added to the RSA Authentication Manager local database. The Authentication Agent record identifies the HTA within its database and contains information about communication and encryption.

The following information is needed to create the Authentication Agent record:

- The HTA hostname
- The HTA management IP address

Perform the following to create an Authentication Agent record:

1. In the RSA Security Console menu select **Access > Authentication Agents > Add New**.
2. Enter the IP address of the HTA.
3. Click the Resolve Hostname button to auto generate the hostname.
4. Click the Save button to create your new Authentication Agent record.

Generating an RSA Configuration File

Perform the following to generate the `sdconf.rec` file from the RSA Authentication Manager:

1. In the RSA Security Console select **Access > Authentication Agents > Generate Configuration File**.
2. Configure/confirm the Agent Timeout and Retries settings.
3. Click the Generate Config File button.
4. Download and extract the `sdconf.rec` file from the zip file.
Configuring the Appliance for RSA SecurID

Perform the following to configure the HTA to use RSA SecurID:

1. Login to the HTA Management Console.
2. Select **Configuration > Two-Factor**.

   The following appears.

3. Click the Choose File button, and navigate to the `sdconf.rec` file you generated from your RSA Authentication Manager.

   **Note:** The Enable SecurID checkbox is grayed out if the `sdconf.rec` file has never been added to the HTA.

4. Click Apply to upload the configuration file.

   A confirmation message appears if the configuration file successfully uploads.

5. Reload the RSA SecurID Configuration page.

6. Select the Enable SecurID checkbox.
7. Click Apply to enable RSA SecurID.
8. Logout from the HTA Management Console.

Creating a New PIN

Set up a new PIN to use when you log into an HTA that uses RSA SecurID.

To create a new PIN:

1. Start the HTA Management Console.
The HTA RSA SecurID login page appears.

![HTA RSA SecurID login page](image)

*Figure 3-13  HTA RSA SecurID login page*

2. Enter the following information:
   - Login—Enter your AD account username.
   - RSA Passcode—Enter the RSA SecurID token (autogenerated from your RSA SecurID device) in this field.

3. Click Login.

You are prompted to enter a new PIN number to use for future HTA logins.

![Change RSA SecurID PIN page](image)

*Figure 3-14  Change RSA SecurID PIN page*

4. Enter your new PIN, and reenter it to confirm.
5. Click OK.

A message appears indicating your PIN has been updated.

![RSA SecurID PIN updated page](image)

*Figure 3-15  RSA SecurID PIN updated page*

You can now login again using your AD account username and your new RSA Passcode.
The RSA Passcode is a concatenation of your new PIN and a newly-generated RSA SecurID token (from software or device). Do not use the same token you used when creating your PIN.

Access to the HTA via the vSphere Client, SSH, or HTTP is supported using your RSA SecurID credentials.

Contact your RSA administrator if you need to change your RSA SecurID PIN.

**CA AuthMinder**

Configuring the HTA to use CA AuthMinder authentication consists of the following tasks:

1. Configuring the Appliance for CA AuthMinder
2. Generating a one-time password to login to the HTA

**Configuring the Appliance for CA AuthMinder**

Perform the following to configure the HTA to use CA AuthMinder:

1. Login to the HTA Management Console.
2. Select Configuration > Two-Factor. (See Figure 3-11.)
3. Open the CA AuthMinder tab.

![Figure 3-16 Configuration > Two-Factor - CA AuthMinder tab](image)

4. Select the Enable CA ArcotID OTP Authentication checkbox.
5. Enter the following information:
   - CA AuthMinder HostName—The IP address or fully qualified hostname of the CA AuthMinder authentication server.
   - CA AuthMinder Port Number—The CA AuthMinder authentication server port number. Default is 9742.
   - Organization Name—The organization name configured in the CA AuthMinder authentication server.
   - CA ArcotID OTP Token Length—The length of the CA ArcotID OTP token. Valid values are 6, 7, or 8. The HTA only supports HOTP type tokens.
   - CA ArcotID OTP Policy Name—The CA ArcotID OTP policy to use.
Consult your CA AuthMinder server administrator for the above information as it must match the CA AuthMinder server configuration.

6. Click Apply.
7. Before you logout from the HTA, open the vSphere Client (or a new HTA Management Console window) and login to the HTA to verify the CA AuthMinder authentication configuration was successful. Enter your AD username and passcode (AD password + CA ArcotID OTP token) to login.

If you can login, CA AuthMinder authentication is successfully configured.

8. Logout from the HTA Management Console.

**Generating a one-time password to login to the HTA**

To generate a one-time password:

1. Open the CA ArcotID OTP client.
2. Enter your PIN.
3. Click Generate Passcode (i.e., CA ArcotID OTP token).
4. Open the HTA Management Console.
5. The HTA CA AuthMinder login page appears.

6. Enter the following information:
   - Login—Enter your AD account username.
   - Password and CA ArcotID OTP—Enter your CA AuthMinder Passcode in this field.

**Note:** The CA AuthMinder Passcode is a concatenation of your existing account password and a newly-generated CA ArcotID OTP token (from software or device).

7. Click Login.

Access to the HTA via the vSphere Client, SSH, or HTTP is supported using your CA AuthMinder credentials.

**Root Password Vaulting**

Root Password Vaulting is a feature that allows the HTA to manage the root password of individual hosts. For each host, the user can select the Root Password Vaulting checkbox on the General tab page when adding or editing hosts—see Managing Hosts on page 44. The HTA will create a new secure root password on the selected host and store it in a
password vault. The HTA automatically rotates or updates the root password on the host on a regular basis (as specified by the Host Password Update scheduled event—see Scheduling Events on page 49).

Note: An Enterprise or appropriate evaluation license is required to implement this feature.

The HTA only supports Root Password Vaulting for ESXi 4.1 update 1 or later hosts. For unsupported ESXi hosts, if the host becomes inaccessible (as determined by assessment or some other host operation that repeatedly caused a connection error or credential error), the recommended user action is to remove the host and add it back to the HTA.

If the HTA becomes unavailable you can recover a root password from an encrypted entry in the HTA log file—see Appendix C, Root Password Recovery for details.

### Prerequisites

Perform the following before enabling Root Password Vaulting:

- Set the HTA Recovery Passcode. The Recovery Passcode is used to provide an emergency mechanism to recover root passwords if the HTA is not available.
- Configure an external Syslog server (highly recommended). In the unlikely event that the HTA becomes unavailable, accessing the HTA log file from the external Syslog server is the only mechanism for recovering a root password.

### Set Recovery Passcode

When the passcode is changed, the new passcode immediately overrides the current passcode and the root account credentials in the log file are re-encrypted. The root password is rotated on hosts with Root Password Vaulting enabled.

To set the Recovery Passcode:

1. Select Configuration > Root Password Vaulting in the HTA Management Console.

2. Enter a Recovery Passcode, and retype to confirm.
3. Click Apply.

The Recovery Passcode is now set and you can enable Root Password Vaulting on your HTA managed hosts.
Enable Root Password Vaulting

Note:
Root Password Vaulting can only be enabled for a host after it has been added and configured.

To enable root password vaulting:
1. Select **Compliance > Hosts** in the HTA Management Console.
2. Click a host in the list.
3. Select the **Root Password Vaulting** checkbox on the **General** tab.
4. Enter the root credentials of the selected host when prompted.
5. Click OK to save your settings.

Once you've enabled root password vaulting, a key ( giovanni ) icon is displayed next to the
hostname on the Hosts summary page.

Request a Temporary Root Password

Once Root Password Vaulting is enabled for the host, an authorized user can request a
temporary root password to access the host.

To request a temporary root password:
1. Open the **Compliance > Hosts** page.

2. Select the checkbox next to the host for which you want to request a temporary root password.

3. Click Issue Password.

4. The HTA prompts you to enter the following information to issue a new temporary root password for the selected host:
   - **Reason**—The reason for the request (e.g., enter the change management ticket, or other tracking information).
   - **Expiration**—The amount of time (in hours) before the temporary root password expires. The minimum expiration period is one hour and the maximum is 24 hours.

5. Click Issue Password.

A User ID and Temporary Password will appear on the screen and also added to the log.
Note: You have two minutes to accept the temporary root password for the designated host. Write down the password or copy the password to your clipboard and paste it into a text editor.

6. Click OK to activate the temporary password.

![HTA login credentials verification](image)

Figure 3-23 HTA login credentials verification

7. At the prompt, enter the credentials you use to log into the HTA and click OK.

   The Hosts summary page appears if the password is issued successfully. Otherwise, the Issue Temporary Password page appears where you can request the password again after 2 minutes.

   Once your host has a temporary root password it can be accessed out-of-band of the HTA until the password expires. To test this, connect to the Service Console via IPKVM, IPMI, etc., and confirm that the temporary root credentials are valid. Also, if you have an additional IP address assigned to your host that the HTA is not managing you can access your host from this second IP address.

   When a temporary root password expires, the HTA automatically replaces the temporary password with a new random secure password.

Note: When Root Password Vaulting is enabled, the HTA does not support SSH login using root credentials to a protected host in Router Mode or using PIP in Mapped Mode. However, other AD users can still login with an SSH session to the protected host through the HTA.

Cancel a Temporary Root Password

To cancel a temporary root password:

1. Open the Compliance > Hosts page.
2. Select the checkbox next to the desired host for which you want to cancel a temporary password.
3. Click Cancel Password.

When a cancel password request is made, the HTA replaces the temporary password with a new random secure password.

In the unlikely event the HTA becomes unavailable, and you need to access an HTA managed host during that time with root credentials, you can recover the root password from an encrypted entry in the HTA log file—see Appendix C, Root Password Recovery for details.

Managing Hosts

You can perform various management tasks on HTA hosts, such as add additional hosts to the HTA, or modify and remove existing HTA hosts.

Adding Hosts to the HTA

To add a new host:

1. From the HTA Management Console, select **Compliance > Hosts** to open the Hosts page.

2. Click Add.

   The HTA Add Host Wizard appears. This wizard sequences through a series of steps to specify a host to add.

3. Complete the Add Host Wizard.

   Refer to the *HyTrust Appliance Installation Guide* for more information on adding hosts to the HTA.
Modifying HTA Protected Hosts

To modify an HTA protected host:
1. From the HTA Management Console, select Compliance > Hosts to open the Hosts page (see Figure 3-25).
2. Click on the host in the Hosts column that you want to modify.
3. Make your changes in the Host Details page.
4. Click OK to save the changes.

Removing HTA Protected Hosts

To remove an HTA protected host:
1. From the HTA Management Console, select Compliance > Hosts to open the Hosts page (see Figure 3-25).
2. Select the checkbox next to the host(s) that you want to remove.
3. Click Remove.

Configuring a Golden Host

As part of a host security posture configuration you can select to replicate the host networking configuration and/or host firewall configuration for consistency, for example, virtual switches, port groups, and physical network interface cards (pNICs). To do this you must designate one ESX host as the Golden Host.

To configure a Golden Host:
1. Open the Host page (Compliance > Hosts).
2. Click on the name of the host you wish to make the Golden Host.
3. Open the Advanced tab.

![Figure 3-26 Compliance > Hosts > Edit Host page - Advanced tab](image)
4. Select the Golden Host checkbox.
5. Click OK.

Now you must run the `vswitch_update` test from the list of available tests and remediation options to replicate the Golden Host configuration settings on the other hosts.

**Configuring Intel TXT**

Comprehensive hardware-based trust can be established utilizing the Intel® Trusted Execution Technology (Intel® TXT), an Intel Xeon processor 5600 series-based hardware platform, and a managed ESXi host running vSphere 4.1 update 1.

The following items are required before this feature can be implemented:

- An Enterprise or appropriate evaluation license
- Hardware and BIOS with Intel TXT support
- Special vCenter Server settings

The HTA can establish platform trust by verifying the correct bootable image of VMware vSphere with the help of Intel TXT on the server platform. Platform trust can also be re-verified at any time and the policies enforced by the HTA automatically adjust based on the individual trust status of each hypervisor / ESXi host.

Administrators can configure expected Trusted Platform Module (TPM) digest values for every build/patch of the VMware ESXi host. When the ESXi host undergoes a trusted launch, it is able to affirm that the server TPM platform configuration register (PCR) values are genuine. If the TPM digest value known to the HTA matches the TPM value generated at boot time for a given ESXi host, the hypervisor acquires a **Trusted** status. However, if the TPM digest values are mismatched, the hypervisor acquires an **Untrusted** status. In cases where the TPM digest value is unknown or unsupported, no labels or icons are applied.

**Enabling Misc.enabledTboot in vCenter Server**

Enable the dynamic launch of the VMkernel using TPM with an advanced configuration option, `enableTboot`, in the vSphere Client. This is referred to as Dynamic Root of Trust for Measurement (DRTM). By default, the use of DRTM for measuring VMkernel is disabled.

To enable Misc.enabledTboot:

1. Open the vSphere Client for your host.
2. On the Configuration tab select **Software > Advanced Settings > Misc.**

3. Set the **Misc.enableTboot** parameter to 1.
4. Reboot the host and verify it boots into trusted mode.
   a. Use the Managed Object Browser tool to verify the **vmware-vmkernel** object has **HostTpmDigestInfo** under the ESXi host **HostRuntimeInfo**.

   **Note:** If TPM is present on a system but disabled in the BIOS, the following error message may appear: **Error loading TPM.** This is expected behavior and you can safely ignore the error message.

**Establishing Host Trust in Appliance**

To establish host trust in the HTA:

1. From the HTA Management Console, select **Configuration > Trusted Execution** from the menu.
2. Click the proper patch level from the list of Trusted Builds.
3. Enter the known TPM digest value.
4. Click OK to save the digest value in the HTA.
5. Open the Compliance > Hosts page.
6. Select the desired Intel TXT ESXi host(s).

**Note:** The actual digest value that was read from the host hardware registers can be seen in the HTA logs. The digest value (which is displayed in a different format) can be seen from the vCenter Server Managed Object Browser (MOB). Converting the digest value may be required before entering it into the HTA.

7. Click Update Trust to establish the trust relationship between the known TPM digest value in the HTA and the TPM digest value generated at boot time for each ESXi host.

As shown in the figure below, the hypervisor acquires the Trusted Host (🔒) icon, indicating that the TPM digest values match.
If the TPM digest values do not match, an Untrusted Host ( ) icon appears. In addition to the Trusted Host ( ) icon, trusted policy labels also appear in the Resource Tree (found in the Policy > Resources menu) for each trusted host in the environment.

### Scheduling Events

You can create a scheduled event to run a defined compliance security template on one or more hosts at a specific time (or at a specific interval)—see Host Configuration Templates on page 70. When the HTA executes a scheduled event with a security template, the security template (with all its individual subtests and operations) will run on each assigned host.

**Note:**

Scheduled Events are restricted by host type. If you assign an ESXi template to a scheduled event only ESXi hosts can be added to that event.

You can view the currently scheduled HTA events from the Compliance > Scheduled Events page.

**Figure 3-33 Scheduled Events page**

By default, the following events are enabled:
Appliance Configuration

Scheduling Events

- **Refresh vCenter plug-in data**—Refreshes the plug-in application information from all protected vCenter Servers.
- **Get Host IP address changes**—Updates host IP address changes to all other protected hosts.
- **Update hosts passwords**—Updates the managed passwords for protected hosts.

By default, the following events are disabled:
- **Get vCenter events**—Updates the log with events from all protected vCenter Servers.
- **Get DRS resource changes**—Updates the policy to include resource changes resulting from a Distributed Resource Scheduler (DRS) activity.

### Adding Scheduled Events

To add a new scheduled event:

1. Click the Add button on the Scheduled Events page.

   ![Add Scheduled Event page](image)

   **Figure 3-34 Add Scheduled Event page**

2. Fill in the details for the scheduled event. The following settings are available:
   - **Name**—The name for the scheduled event.
   - **Description**—A description for the scheduled event.
   - **Start**—The date and time to start the scheduled event. Enter the date or click the calendar button and choose a date, and enter the time. The default is the current date and time on the HTA.
   - **Interval (Minutes)**—The amount of time in minutes between runs of this scheduled event. The valid range of values is 1–525600 (1 year).
   - **Template**—The security template to use for the scheduled event.
   - **Enabled**—Enable (selected) or disable (deselected) the scheduled event.

3. Add hosts to run this scheduled event on in the *Hosts* section at the bottom of the page:
a. Click the Add button to open the Add Host to Scheduled Event page.

b. Select the hosts to run this scheduled event on. (Only hosts matching the selected template type appear in the list.)

c. Click OK.

4. Click OK to save the scheduled event.

**Editing Scheduled Events**

You can enable or disable a scheduled event as well as change its start time and interval. To edit a scheduled event:

1. Click on the event name in the Scheduled Events list.

2. You can edit the following settings:
   - **Start**—The date and time to start the scheduled event. Enter the date or click the calendar button and choose a date, and enter the time.
   - **Interval (Minutes)**—The amount of time in minutes between runs of this scheduled event. The valid range of values is 1–525600 (1 year).
   - **Enabled**—Enable (selected) or disable (deselected) the scheduled event.

3. Click OK to save your changes.
Deleting Scheduled Events

To delete a scheduled event:
1. Select the checkbox next to the scheduled event(s) you want to delete.
2. Click Delete to remove the scheduled event:

---

**Note:** You can also disable the scheduled event (deselect the Enabled checkbox) instead of deleting it, in case you decide you want to use it again at a later time.

---

Retrieving vCenter Server Events

While the HTA has a comprehensive view of all user initiated vSphere operations in the virtual infrastructure, importing vCenter Server events may be useful for completeness and to include automated events (e.g., DRS).

To enable the HTA to retrieve events from a vCenter Server:
1. Open the **Compliance > Scheduled Events** page (see Figure 3-33).
2. Click on the **Get vCenter events** scheduled event name.
3. Confirm the interval setting.
4. Select the Enable checkbox.
5. Click the OK button to save the scheduled event.
6. Open the **General > Log Viewer** to view vCenter Server events. All vCenter Server log messages start with ARC0035I VC (see Figure 7-2).

Configuring Notifications

You can configure the HTA to notify an administrator by email or SNMP if a service or resource becomes unavailable.

---

**Note:** It is highly recommended that you configure monitoring services, especially when using High Availability (HA).

---

SMTP notifications and SNMP monitoring operate the same as on Linux-based systems. The following is a list of notifications an administrator may receive:

**Table 3-1 Notifications**

<table>
<thead>
<tr>
<th>Message</th>
<th>ID</th>
<th>SNMP OID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Transition to Disabled</td>
<td>MON0000</td>
<td>1.3.6.1.4.1.33095.0.1100</td>
<td>The appliance indicates that a monitored service is now disabled.</td>
</tr>
<tr>
<td>Monitor Transition to Healthy</td>
<td>MON0001</td>
<td>1.3.6.1.4.1.33095.0.1101</td>
<td>The appliance indicates a service or resource has returned to normal operation.</td>
</tr>
</tbody>
</table>
To enable and configure SMTP notifications and SNMP monitoring:

1. Open the **Configuration > Monitoring** page.

2. For SMTP Notifications:
   a. Select the **Enable SMTP** checkbox and fill in the **SMTP Host** field.
   b. Select the **Enable Monitoring** checkbox and fill in the from and to email addresses.

3. For SNMP monitoring, select the **Enable SNMP** box and fill in the **SNMP Server** and **SNMP Community String** fields.

4. Click Apply to save your settings.

### Managing Certificates

The HTA uses different certificates for the Logging service and the HTA Web Application service. The Logging service is for Syslog and the Web Application service is for proxies and the HTA Management Console. If needed, you can install your own certificates generated by a certificate authority (CA) for these services.
Open the **Configuration > Certificates** page to view the currently installed certificates.

The columns that appear indicate the owner, issuer, and expiration date for each installed certificate.

### Generating a Certificate

To generate a certificate or a Certificate Signing Request (CSR):

1. Select a service (e.g., Web Application) from the Certificates page list.

   ![Certificate details page](image)

   **Figure 3-39 Certificate details page**

   This page shows the certificate details for the selected service.

2. Click the Generate CSR button.

   ![Generate Certificates page](image)

   **Figure 3-40 Generate Certificates page**
3. Fill in the Common Name and Country, and any other fields that apply to your organization.

4. Click OK.

Once the CSR is generated, you can copy it into an email and submit it to a Certificate Authority (CA) or paste it into the CA console to have it issue a certificate.

![Certificate CSR Data page](image1)

**Figure 3-41  Certificate CSR Data page**

5. Submit the CSR Data to your CA.

You can install the signed certificate after you receive it from your CA.

### Installing a Signed Certificate

Before you can install a certificate you must submit a request and obtain a signed certificate from your CA—see Generating a Certificate on page 54. Once you have a signed certificate you have two options to install it, (1) copy and paste the contents of the certificate file, or (2) upload the certificate file directly.

To install a signed certificate:

1. Select a service (e.g., Web Application) from the Certificates page list.

![Certificate Details page](image2)

**Figure 3-42  Certificate details page**
2. Click the Install button.

![Install Certificate page]

3. Copy and paste the certificate data in the Certificate Data field. You can also use the Import tab to upload your certificate file.

4. Click OK.

Installing a Third-party Root Certificate

You can install a root certificate from any third-party Certificate Authority (public or private) if not already pre-installed in the HTA.

To install a third-party root certificate:
1. Open the Certificate Authorities tab.

![Configuration > Certificates - Certificate Authorities tab](image)

2. Click the Install button.

![Install Certificate](image)

3. Enter the full file path and name in the Upload Certificate field, or click Browse to select a CA certificate file to upload.
4. Click OK.

### Changing Password Requirements for ascadminuser

The local HTA administrator account (ascadminuser) password complexity is based on the default settings built into the HTA operating system (CentOS). You can enhance these default settings if your environment requires additional password complexity.

To change the ascadminuser password requirements:

1. Open the **Configuration > Password Requirements** page.

#### Figure 3-46  Password Requirements configuration page

2. Make your changes using the following fields:
   - **Minimum Length**—Set the minimum password length. Default is 8.
   - **Minimum Uppercase**—Set the minimum number of required uppercase characters.
   - **Minimum Lowercase**—Set the minimum number of required lowercase characters.
   - **Minimum Digits**—Set the minimum number of required digits (0-9).
   - **Minimum Non-Alphanumeric**—Set the minimum number of required non-alphanumeric characters.

3. Click Apply to save your changes.

#### Note:
After changing password requirements you must change your ascadminuser password to meet the new requirements.

### Changing the ascadminuser Password

To change your ascadminuser password:

1. Login to the HTA from the Virtual Machine Console Window within vCenter Server or via SSH using your ascadminuser credentials.

2. From the command prompt, type:
   ```
   passwd
   ```
   to change your password.
3. Enter your new `ascadminuser` password. The new password must conform to the newly defined password requirements.

**Third Party Configuration**

The HTA integrates with several third party products, including:

- Trend Micro Deep Security Manager
- CA Access Control for Virtual Environments

Contact HyTrust Support to obtain installation and configuration information for supported third party products.

**vCenter Server Plugin**

The HTA vCenter Server Plugin allows users to access some HTA functionality (e.g., host assessment) directly from the vSphere Client.

An HTA administrator uses the HTA Management Console to register or unregister the HTA vCenter Server Plugin for a specific vCenter Server.

**Registering the vCenter Server Plugin**

To register the HTA vCenter Server Plugin:

1. Open the **Configuration > vCenter Plugin** page.

2. Select **Register Plugin** from the Operation drop down menu.

3. Fill in the following fields:
   - **vCenter Server**—The IP address or FQDN of the vCenter Server.
   - **vCenter Username**—The vCenter Server username with an Administrator role.
   - **vCenter Password**—The password for the vCenter Server.

4. Click Go.
From the vSphere Client, login to the vCenter Server and confirm that the HyTrust tab is now available in the vSphere Client.

If the HyTrust tab is not visible, confirm that the HTA vCenter Server Plugin was installed properly in the Plug-in Manager (Plug-ins > Manage Plug-ins) within the vCenter Server.

From the HyTrust tab, you can click the General, Hosts, Policy, Configuration, Maintenance and Help menu items to perform the same operations as available in the HTA Management Console.

**Note:**

The privilege level for the user logged in to the vSphere Client determines the available menu items.

**Unregistering the vCenter Server Plugin**

To unregister the HTA vCenter Server Plugin:
1. Open the **Configuration > vCenter Plugin** page.

![Configuration > vCenter Plugin page](image)

*Figure 3-49  Configuration > vCenter Plugin page*

2. Select **Unregister Plugin** from the Operation drop down menu.
3. Click Go.
4. Log out from the vSphere Client and log back in to fully remove the HTA tab from the vSphere Client.
CHAPTER 4

Hardening Hypervisors

This chapter contains the following sections:

- Host Compliance
- Assessing ESX and ESXi Hosts
- Remediating ESX and ESXi Hosts
- Assessment History
- Host Configuration Templates

Host Compliance

You can view a list of HTA-protected hosts on the Compliance > Hosts page in the HTA Management Console along with the corresponding compliance scores based on the security compliance template assigned to a host.

![Figure 4-1 Compliance Hosts page](image)

On the Hosts page you can view details about a specific host configuration, assess or remediate hosts based on an assigned template, issue or cancel a temporary host password—see Root Password Vaulting on page 39, update trust on an Intel TXT enabled ESXi host—see Configuring Intel TXT on page 46, and add or remove hosts from HTA protection—see Managing Hosts on page 44.

The following information is provided in the various columns on the Hosts page:

- Hosts—The name of the host. Click a host to view/edit its settings.
- Host Type—The host type (ESX Host, ESXi Host, vCenter Server, etc.).
Hardening Hypervisors

Assessing ESX and ESXi Hosts

- Patch Level—The host version.
- Default Template—Displays the security compliance template assigned to the host.
- Results—Click the Details link to access the results of all tests performed on a selected host. (See Assessing ESX and ESXi Hosts on page 64.)
- Compliance—Shows the host compliance percentage. This refers to the number of operations or tests that passed assessment. The calculation is based on the default template for the host and includes all runs over the past week. For example, in a given template, if 10 tests ran and 8 passed, the compliance shows 80%.

The following buttons are available on the Hosts page:

- Add—Opens the Add Host Wizard which you can use to add a new ESX or ESXi host, vCenter Server, Nexus 1000V VSM, or UCS Manager to the HTA—see Adding Hosts to the HTA on page 44.
- Edit—Opens the Edit Host page where you can change the configuration settings for the selected hosts. You can also click on the hostname in the Hosts column if you want to change the configuration settings for a single host.
- Remove—Removes the selected host(s) or vCenter Server(s) from HTA protection.
- Assess—Runs all tests contained in the compliance template on the selected ESX or ESXi host(s)—see Assessing ESX and ESXi Hosts on page 64.
- Remediate—Runs all tests contained in the compliance template on the selected ESX or ESXi host(s) and attempts to fix any issues encountered—see Remediating ESX and ESXi Hosts on page 66.
- Update Firewall—Refreshes the firewall rules on the HTA for each of the selected hosts.
- Export as CSV—Exports the test results for the selected host(s) to a comma-separated-value (CSV) file. You can also specify a time frame to export historical Assess Remediate Compliance (ARC) test results performed for each selected host.
- Issue Password—Issues a temporary one-time root password after the Root Password Vaulting feature has been enabled—see Request a Temporary Root Password on page 41.
- Cancel Password— Cancels an issued temporary one-time root password. The HTA will automatically replace the temporary root password with a new random secure password and store the new password—see Cancel a Temporary Root Password on page 43.
- Update Trust—Compares the TPM digest value known to the HTA and the TPM value generated at boot time for the selected host. If the digest values match the HTA assigns a Trusted Host icon to the host—see Establishing Host Trust in Appliance on page 47.

Assessing ESX and ESXi Hosts

Compliance template operations or tests on protected hosts can occur as scheduled events or ad hoc. Ad hoc tests are performed immediately whereas scheduled tests are performed at a specified date and time in the future. See Scheduling Events on page 49 for information on scheduling template events.

To perform an ad hoc ESX/ESXi host assessment:

1. Open the Compliance > Hosts page.
2. Select one or more hosts and click the Assess button.
All the tests contained in the compliance template will run for the selected host(s). After the tests finish the HTA updates the information in the Compliance column for the selected host(s).

3. Click the Details link in the Results column to display the test results for a specific host.

The HTA displays all possible tests that could run for the specific host type along with the most recent Pass/Fail test results.

The Test Results page shows results not only for tests performed by the last assessment run (for tests in the template currently assigned to a host) but also for any other tests that may have been run within the same 1-week time period for that host. For example, if test A ran as part of the CIS template that ran last week, and test B ran as part of the PCI template that ran yesterday, both tests will appear in the displayed test results. The Date column displays the date and time a test last ran.

**Figure 4-2** Test Results page

Dates and times displayed on the Test Results page are shown in the local date and time set on the client computer (i.e., the local machine where the browser
window is running the HTA Management Console).

4. If desired, click the Export as CSV button to output the test results to a comma-separated-value (CSV) file. You can do this either on the Test Results page or the Hosts page.

You can select individual tests on the Test Results page and click the Assess button to create a new template, run it, and display the results of those tests (overlaying existing test results displayed on the Tests Results page). The new template cannot be saved and does not show up in the list of available templates unless you select the desired test results from the Test Results page and click the Copy button. On the Save As Custom Template page, name your new template and click OK to save your settings.

**Remediating ESX and ESXi Hosts**

Remediation performs the same tests as an assessment but also attempts to address any deviations from the compliance template encountered when the tests are run.

To perform an ad hoc ESX/ESXi host remediation:

1. Open the **Compliance > Hosts** page.
2. Select one or more hosts and click the Remediate button.

   All the tests contained in the compliance template will run for the selected host(s). After the tests finish the HTA updates the information in the Compliance column for the selected host(s).

3. Click the Details link in the Results column to display the test results for a specific host (see Figure 4-2).

   The HTA displays all possible tests that could run for the specific host type along with the most recent Pass/Fail test results.

   The Test Results page shows results not only for tests performed by the last remediation run (for tests in the template currently assigned to a host) but also for any other tests that may have been run within the same 1-week time period for that host. For example, if test A ran as part of the CIS template that ran last week, and test B ran as part of the PCI template that ran yesterday, both tests will appear in the displayed test results. The Date column displays the date and time a test last ran.

   **Note:** Dates and times displayed on the Test Results page are shown in the local date and time set on the client computer (i.e., the local machine where the browser window is running the HTA Management Console).

4. If desired, click the Export as CSV button to output the test results to a comma-separated-value (CSV) file. You can do this either on the Test Results page or the Hosts page.

You can select individual tests on the Test Results page and click the Remediate button to run and display the results of those tests (overlaying existing test results displayed on the Tests Results page).

To create a new template and save it in the list of available templates, select the desired test results from the Test Results page and click the Copy button. On the Save As Custom Template page, name your new template and click OK to save your settings.
Assessment History

The Compliance > History page allows you to view or audit historical HTA compliance testing information. The four tabs available on the compliance history page (Summary, Hosts, Details, and Templates) enable you to view all compliance template checks and tests.

From the Hosts and Details tabs, users can drill down to pass/fail test results for specific hosts or templates and export the results in CSV format.

Summary

The Summary tab shows the historical overall compliance percentage of protected hosts for a recurring time period.

Each row represents the summary for a 7-day period. The end of each period is dynamic and is defined at the time the Compliance History report was generated. Rows for each time period are displayed in descending date order.

The following columns are displayed:

- **Date/Time**—The date and time when the report was generated.
- **Hosts**—The total number of hosts.
- **Protected Hosts**—The number of protected ESX and ESXi hosts.
- **Compliance**—The aggregate compliance percentage based on the tests in the default template assigned to each host. This value is calculated by dividing the number of tests that passed by the total number of tests run in the 7-day period.

Hosts

The Hosts tab shows the percentage pass rate for each host, for all compliance tests in the default template assigned to that host.

The following columns are displayed:
Hardening Hypervisors

Assessment History

- **Name**—The name of the host. Click a name link to display the Compliance Detail page that shows a list of all assessments for that host. See Compliance Detail on page 68.
- **Compliance**—This column shows the calculated compliance value for each host by using its pass/fail counts for every assessment, regardless of the template. The HTA uses all assessments run for that host.

**Compliance Detail**

The Compliance Detail page shows detailed compliance information for the selected host.

---

**Figure 4-5 Compliance Host Detail page**

The following columns are displayed:

- **Date/Time**—The date and time when the information was calculated. Click a link in this column to display the Compliance Test Results page (see Figure 4-6) for the assessment which you can export in CSV format.
- **Template**—The template against which the host assessment was run.
- **Host**—The host for which the report applies.
- **Compliance**—The compliance percentage for the host. This value is calculated by dividing the number of tests that passed by the total number of tests run during the assessment.

---

**Figure 4-6 Compliance Test Results page**
Details

The Details tab shows a list of all assessments for all hosts, giving the compliance percentage for each template execution, ad hoc (manually, by user) or scheduled.

![Compliance History - Details tab](image)

The following columns are displayed:

- Date/Time—The date and time when the report was generated. Click a link in this column to display the Compliance Test Results page (see Figure 4-6) which you can export in CSV format.
- Template—The assigned template which was used for host assessment.
- Host—The host for which the report applies.
- Compliance—The compliance percentage for the host. This value is calculated by dividing the number of tests that passed by the total number of tests run during the assessment. The HTA displays compliance percentage numbers in a separate row for each host if a template run is a result of an event that involves more than one host.

Templates

The Templates tab shows a list of all the security templates, the current number of operations in each template, and the last modified date.

![Compliance History - Templates tab](image)

The following columns are displayed:

- Name—The template name.
- Operations—The number of operations, or tests, contained in the template.
- Last Modified—The date and time the template was last changed.
Hardening Hypervisors
Host Configuration Templates

Host Configuration Templates

You can assign a specific security compliance template to each host from the Add/Edit Host page. You can select Compliance > Templates to view the currently available templates.

Templates available out of the box allow you to assess your virtual infrastructure against Center of Internet Security benchmarks (CIS, CIS-ESXi), PCI DSS recommendations (PCI, PCI-ESXi), VMware security hardening guidelines (VMware_SH, VMware_SH4, Vmw4-ESXi), and SOX (SOX, SOX-ESXi) compliance.

For more information refer to the following standard setting organizations websites:

- **CIS**: [http://www.cisecurity.org/](http://www.cisecurity.org/)
- **PCI DSS**: [https://www.pcisecuritystandards.org/](https://www.pcisecuritystandards.org/)

From the Templates page you can click on a specific template name to display the Edit Template page where you can view all the individual checks and tests included in that template. You can also click the Add button to create a customized set of checks and tests.

The original templates that ship with the HTA are read-only. If you wish to modify one of the read-only templates, you must first Copy the template and assign a unique name to your custom template. After your new template is successfully added you can add or remove operations, set custom parameters, and determine the assignment (assess or remediate) for each test.

Some tests that are part of the original read-only templates may be configured as assess only, while others may be configured to remediate the host.

**Note:**
Make sure to review all operations that require parameters before assessing or remediating a host. Parameters can only be assigned in custom templates.

Export Template

To export a template:
1. On the Templates (Compliance > Templates) page, select the checkbox next to the desired template and click the Export/Import button. The Export/Import Templates page appears.

![Image of Export/Import Templates page]

**Figure 4-10  Export / Import Templates page**

2. Click the Click to Export button.
3. Save the file to your local host.

**Import Template**

To import a new template:

1. Click the Export/Import button. The Export/Import Templates page appears (see Figure 4-10).
2. Enter the template file you want to import in the File to Import field, or click the Browse button to find the file you want to import as a new template.
3. Click Import.
Hardening Hypervisors
Host Configuration Templates
Creating and Deploying Access Policies

This chapter contains the following sections:

- Overview
- Policy Definitions and Behavior
- Separation of Duties
- Policy Interaction
- Example Policies

Overview

Before you create and deploy access policies on your virtual infrastructure you need to confirm that the HTA is protecting the vCenter Server and all your imported hosts. Refer to the *HyTrust Appliance Installation Guide* for assistance importing a vCenter Server, adding a host, or protecting these resources.

When the initial vCenter Server import is performed, the vCenter Server object structure is added to a new draft policy which is auto-deployed by the HTA.

Any time a new virtual machine is created or a new host is added, the new object is automatically added to the HyTrust policy and the deployed policy is enforced on the new object. This is referred to as a Structure Changing Operation (SCO). A multi-user locking mechanism safeguards against conflicts in policy changes.
Creating and Deploying Access Policies

Overview

The HTA Management Console History (Policy > History) page provides access to policy Resources, Rules, Roles, RuleSets, Labels, and History.

Figure 5-1 Policy > History page

The History page displays the active or deployed policy, draft policy in the process of being modified, and archived policy versions.

Note: HyTrust recommends that you schedule manual policy changes, such as creating new rules, for times when change control on the virtual infrastructure is enforced and no new virtualized objects are being created.

You can export policies as an XML file by selecting the checkbox next to the desired policy and pressing the Export button. You can also click a Policy link to view more details about it, such as, the entire hierarchy of virtual infrastructure objects, rules, roles, and authorizations. You can apply these policies to a selected ESX host or vCenter Server installation. You can also import policies from an ESX host or vCenter Server.
Creating and Deploying Access Policies

Overview

Viewing the Current Policy

An HTA Policy is a combination of all rules defined in the system. The Deployed policy is the policy currently in effect. Click the Deployed policy link on the History page to open the Policy Resources page where you can view the current policy.

![Policy Resources for Policy Deployed](image)

Figure 5-2 Deployed Policy Resources page

Changing the Current Policy

Note: Most pages under the Policy menu include both a Create Draft and Deploy button. If a particular button on any of the Policy submenu pages is disabled, such as the Add, Delete, or Discard Changes button, be sure to click the Create Draft button first.

Note: If changes were made within your virtual infrastructure where a user needed access and went around the HTA, you must manually refresh the policy resource tree by clicking the Refresh button before creating a new policy definition—in Draft mode the Refresh button is disabled.

To make a change in the deployed policy, such as adding a new rule to the vCenter Server:
1. Open any Policy page.
2. Click the Create Draft button. This copies the Deployed policy to a Draft policy.
3. Make your desired changes to the Draft policy using the various policy pages.

Note: Ensure Draft is selected in the Type or Policy drop-down list on the policy pages when making your changes.

4. Click the Deploy button to replace the current Deployed policy with the Draft policy.

Note: An archived policy is created from the previous Deployed policy. Archived policies exist as an audit trail only. There is no mechanism to roll back to an archived policy.
Creating and Deploying Access Policies

Policy Definitions and Behavior

This section provides details on the policy definitions within the HTA.

Policy Resource

A policy resource is any object that is part of the Policy Resource tree. Select Policy > Resources to view the objects that make up the Policy Resource tree.

![Policy Resources](image)

Figure 5-3 Policy > Resources page

**Note:** Draft Rules, RuleSets, and Labels show up in the Policy Resource tree; however, they do not take effect until the draft policy is deployed.

Roles

Roles are collections of privileges or permissions that define authorized operations, usually defined along the same lines as roles or duties that users perform within an organization. A Role may also become an attribute of a Rule.
Roles may be modified, added, and deleted from the **Policy > Roles** page.

### Domain User Group

After converting to Directory Service mode the HTA uses its service account to query group membership in the Active Directory (AD). When creating a rule, an existing domain user group can be mapped to an HTA role. Within AD, members of the domain user group must be manually assigned before the rule can be utilized.

### Rules

Rules are relationships between AD domain user groups, objects, and entitled operations for a specific role. Rules may be added, deleted, assigned to single or multiple resources, or assigned to RuleSets.

Default rules are always assigned to the root of the resource tree and affect all child objects in the tree.
You use the **Policy > Rules** page to perform single or multiple Rule assignment to Resources or RuleSets.

### Constraints

Rules may have specific constraints assigned, such as:

- **Client Protocol**—access restricted by SSH, vSphere Client or HTTPS
- **Client IP Range**—access restricted by IP address range.
- **Client IP Match**—access restricted by a single IP address.
- **Match VM Label(s)**—access restricted by virtual machine label.
- **Match Host Label(s)**—access restricted by host label.
- **Match Label(s) by Name**—access restricted by any label.
- **Match Network Label(s)**—access restricted by network label.
The Match Network Label(s), Match Host Label(s), Match Label(s) by Name, and Match VM Label(s) constraints only take effect after the corresponding Labels are assigned to the proper policy resource.

If more than one constraint exists in a given rule, then all constraints must be satisfied before the operation can proceed.

To assign a constraint to a rule:
1. Open the Rules page (see Figure 5-5).
2. Click on the desired rule name.
3. On the Edit Rule page, click the Add button to create your constraint.
4. Select the Constraint Type.
5. Complete the required information.
6. Click OK.

The required information depends on the selected constraint.

RuleSets

RuleSets are a collection of rules, that when present disable direct rules assigned to an object. Each RuleSet contains a rule or set of rules, each with its own domain user group, role, and constraint. Each RuleSet can also be assigned to one or more policy resources.

To create and assign a RuleSet:
1. Open the Policy > RuleSets page.
2. Click the Add button to create a RuleSet.
3. Once the RuleSet has been created, select the checkbox next to the desired RuleSet and click the Assign Rules button.
4. Select the rule(s) and click the OK button to save your settings.

If a policy resource includes more than one RuleSet, each RuleSet is evaluated independently (i.e., the conditions of only one must be met for the operation to proceed).

By default, RuleSets always propagate down the policy resource tree.
Creating and Deploying Access Policies
Policy Definitions and Behavior

Note: If a policy resource is associated with a RuleSet without a rule, then ALL ACCESS to that policy resource is denied. Likewise, since a deployed RuleSet creates a new policy resource domain for a given object, it is highly recommended that you also include a rule within each RuleSet that contains the HT_SuperAdmin domain user group and the ASC_SuperAdmin role.

Note: By default, the CoreAppliance RuleSet does not include SuperAdmin privileges. If SuperAdmins need access to policy objects containing the CoreAppliance RuleSet, add a rule within the RuleSet that contains the HT_SuperAdmin domain user group and the ASC_SuperAdmin role.

Assigning Resources to RuleSets

Perform the following to assign resources to a RuleSet:

1. Open the Policy > RuleSets page (see Figure 5-6).
2. Click the Create Draft button, to create a new draft policy.
3. Select the RuleSet (e.g., CoreAppliance).
4. Click Assign Resources.
5. Select the resource (e.g., HyTrust Appliance Appliance Root) item and click OK. If necessary, use the search field to narrow your search.
6. Click Deploy.

Figure 5-7 Assign RuleSets page
Creating and Deploying Access Policies
Policy Definitions and Behavior

7. Click the RuleSet (e.g., CoreAppliance) to see that the resource (e.g., Appliance Root) appears in the Assigned Resources section.

![RuleSet details page](image)

**Figure 5-8  RuleSet details page**

**Labels**

Labels are used to classify or categorize policy resources. Labels are useful when defining rule constraints. For example, virtual machines can be constrained to start only on the hosts with the correct label (e.g., production).

Use the **Policy > Labels** page to manage labels.

![Policy > Labels page](image)

**Figure 5-9  Policy > Labels page**

There are two built-in labels, **TRUSTED** and **UNTRUSTED**. Although not a requirement, the recommended usage for these two labels is in environments utilizing the Intel TXT platform.

**Note:**
Labels associated with the following constraint types: Network Label Match and Host Label Match should only be assigned to hosts or port groups. Labels associated with the Label Match by Name constraint can be assigned to any object in the policy resource tree. These constraints only take affect after the corresponding Labels are assigned to the proper policy resource(s).
Separation of Duties

The HTA provides the capability to define roles as a collection of privileges on a per role basis, allowing system administrators to control which HTA roles can perform what operations within the virtual infrastructure. This is called separation of duties.

To manage HTA role privileges:

1. Open the Policy > Roles page (see Figure 5-4).
2. Click on the name of the role for which you want to manage.

The Edit Role page appears.

3. Use the checkbox next to a privilege to allow or deny the operation on the specified vCenter managed object type for this role.
   - Deny all operations on the vCenter managed object type.
   - Allow some operations on the vCenter managed object type.
   - Allow all operations on the vCenter managed object type.

4. Click OK to save the changes.
Policy Interaction

The HTA Policy Engine carries out the following workflow when a user performs an operation on a given policy resource:

1. The HTA Policy Engine first looks at the local rule or rules assigned to the resource object.
   - If a true statement is found from the local rule or rules, the requested operation is allowed.
   - If a false statement is found from the local rule or rules, the policy engine walks up the policy tree to the next node and applies the same line of reasoning.
     If a RuleSet is found during the process of walking up the resource tree, the local rule or rules that are shared on the same node as the RuleSet are ignored.
     The policy engine then evaluates the RuleSet.
     - If a true statement is found, the requested operation is allowed.
     - If a false statement is found, the policy engine terminates the user request and the operation is not allowed.

Example Policies

It is recommended that a user with sufficient credentials (i.e., ASC_SuperAdmin role) login to the HTA Management Console to create the policies and perform the tasks described in this section.

Note:
The examples in this section are only meant to provide insight into typical HTA policy scenarios and may not match your exact requirements and environment.

You should be familiar with how to create rules and assign HTA rules and constraints as described previously.

Example 1—Allow DevGroup to Create Virtual Machines on DevCluster Hosts

This example shows how to setup an HTA policy that allows any DevGroup user to create virtual machines (VMs) only on hosts within the DevCluster development cluster.

This also implies that DevGroup users cannot move VMs out of the DevCluster.

Policy Setup

1. Assume that all development users belong to the DevGroup group.
2. Create the necessary rules.
   a. DevRule (DevGroup, AllPriv-Role)

   Note: The AllPriv-Role represents a role with all privileges and can be tailored to a given setup.

   b. DevLogin (DevGroup, BasicLogin)
3. Create the DevCluster cluster (all hosts that are available for use by the development group reside here).
4. Assign the DevLogin rule to the vCenter/HTA.
5. Assign the DevRule to the following resources:
   a. VM folder
   b. DevCluster
   c. Network folder
   d. Datastore folder

**Example 2—Allow Two Different Administrator Groups to Use Separate Host Clusters and Inventory Folders**

This example shows how to setup an HTA policy that allows two different administrator groups to use separate host clusters and inventory folders.

- **AdminGroupA:**
  - Create VMs in FolderA (inventory folder)
  - Create hosts in ClusterA

- **AdminGroupB:**
  - Create VMs in FolderB (inventory folder)
  - Create hosts in ClusterB

**Policy Setup**

1. Assume the user has Login privilege for the vCenter.
2. Assume the following objects are created in the vCenter.
   a. Inventory folders: FolderA, FolderB
   b. Host clusters: ClusterA, ClusterB
3. Create the necessary rules.
   a. RuleA (AdminGroupA, AllPriv-Role)
   b. RuleB (AdminGroupB, AllPriv-Role)
4. Assign the rules.
   a. RuleA to resources ClusterA, FolderA, Network folder, and Datastore folder
   b. RuleB to resources ClusterB, FolderB, Network folder, and Datastore folder

In this setup, an AdminGroupA user can create a VM in ClusterA and FolderA, but cannot move that VM to FolderB or any host in ClusterB.

**Example 3—Allow Two Different Administrator Groups to Manage Separate Virtual Machines Using OS Label**

This example shows how to setup an HTA policy that allows two different administrator groups to manage separate virtual machines.

- **WinAdmin**—Manage all VMs with a WinVM label.
- **UnixAdmin**—Manage all VMs with a UnixVM label.

**Policy Setup**

1. Assume the user has Login privilege for the vCenter.
2. Assign labels based on operating system type.
   a. WinVM—Assign to all VMs with Windows OS.
   b. UnixVM—Assign to all VMs with Unix OS.
3. Create the necessary rules.
a. **WinRule (WinAdmin, AllPriv-Role)**
   
   Add the WinVM label to the following constraints:
   
   - Match VM Label

b. **UnixRule (UnixAdmin, AllPriv-Role)**
   
   Add the UnixVM label to the following constraints:
   
   - Match VM Label

4. Assign the rules.
   
   a. WinRule to the HTA.
   
   b. UnixRule to the HTA.

In this setup, a WinAdmin user can only manage VMs with a WinVM label, and a UnixAdmin user can only mange VMs with a UnixVM label.

---

**Example 4—Segmenting Out Part of the Virtual Machine Infrastructure**

This example shows how to setup an HTA policy that allows two different administrator groups to manage separate virtual machines.

- **PciAdmin:**
  
  - Manage VMs with a PCI label on hosts and networks with a PCI label.

- **SysAdmin:**
  
  - Manage VMs without a PCI label on hosts and network without a PCI label.

**Policy Setup**

1. Assume the user has Login privilege for the vCenter.

2. Assign the PCI label to all VMs, hosts, and port groups to be managed by the PciAdmin group.

3. Create the necessary rules.
   
   a. **PciRule (PciAdmin, AllPriv-Role)**
      
      Add the PCI label to the following constraints:
      
      - Match VM Label
      - Host Label Match
      - Network Label Match

   b. **SysRule (SysAdmin, AllPriv-Role)**
      
      Add the PCI label and select the Exclude... checkbox to the following constraints:
      
      - Match VM Label
      - Host Label Match
      - Network Label Match

4. Assign the rules.
   
   a. SysRule to the HTA.
   
   b. PciRule to the HTA.

In this setup, a PciAdmin user can only mange VMs with a PCI label and a SysAdmin user can only manage VMs without a PCI label.
Example 5—Allow SysAdmin Group to Manage All Objects, But Cannot Move Virtual Machines with PCI Label

This is a special case example that shows how to setup an HTA policy that allows the SysAdmin group to manage all objects, but cannot move VMs with a PCI label to hosts and networks without a PCI label.

Policy Setup

1. Assume the user has Login privilege for the vCenter.
2. Assign the PCI label to all VMs, hosts, and port groups as appropriate.
3. Create the necessary rules.
   a. PciRule (SysAdmin, AllPriv-Role)
      Add the PCI label to the following constraints:
      - Match VM Label
      - Host Label Match
      - Network Label Match
   b. SysRule (SysAdmin, AllPriv-Role)
      Add the PCI label and select the Exclude... checkbox to the following constraints:
      - Match VM Label
      - Host Label Match
      - Network Label Match
4. Assign the rules.
   a. SysRule to the vCenter/HTA.
   b. PciRule to the vCenter/HTA.

In this setup, a SysAdmin user can manage all VMs, but cannot move VMs with a PCI label to a host or network without a PCI label.
Secondary Approval

This chapter contains the following sections:

- Overview
- Configuring Secondary Approval
- Pending Requests
- Request History

Overview

Secondary Approval allows authorized users to configure the HTA to require additional approval before users can perform select disruptive virtual machine operations (e.g., power off a VM, edit VM settings, or move a VM).

Note: An Enterprise or appropriate evaluation license is required to use the Secondary Approval feature.

When a user attempts to perform a vSphere Client operation deemed to require secondary approval, the HTA notifies the requestor that approval is needed, sends an email notification to the approval group who can authorize the request, adds the request to the pending list, and waits for an authorized user to approve or deny the request.

Once a request is approved or denied, the HTA sends an email notification to the requestor, the approver, and, if applicable, the approval group.

Note: Users cannot approve their own requests, even if they are in the approval group (i.e., a different user must approve the request).
Secondary Approval
Configuring Secondary Approval

The following table lists the HTA privileges that specify control of Secondary Approval operations.

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asc.SecondaryApproval.Approver</td>
<td>Allows an HTA user to approve or deny Secondary Approval requests.</td>
</tr>
<tr>
<td>Asc.SecondaryApproval.Configurer</td>
<td>Allows an HTA user to configure Secondary Approval settings.</td>
</tr>
</tbody>
</table>

## Configuring Secondary Approval

The following are required before you can configure Secondary Approval:

- SMTP notifications must be enabled—see **Configuring Notifications** on page 52.
- The HTA must be in Directory Service mode—see **Integrating the Appliance with Active Directory** on page 30.

To configure Secondary Approval:

1. In the HTA Management Console, select **Configuration > Secondary Approval**.

2. Configure the following settings:
   - **Enable**—Enables (selected) or disables (deselected) using Secondary Approval with the HTA.
   - **CC Approvers**—Enables (selected) or disables (deselected) sending an email notification to all users in the approval group when another approves or denies the request.
   - **Default Duration**—The default amount of time, in hours, for a request approval to last (i.e., how long the operation is authorized).

   ![Secondary Approval Configuration](image)

   **Figure 6-1 Configuration > Secondary Approval page**

   **Note:** If the Enable checkbox is not visible, a message indicating that either AD or SMTP needs to be configured will appear.
Email Address (FROM)—The email address that displays in the From field when a Secondary Approval email notifications is sent.

3. Click Apply.

4. If Secondary Approval is enabled, a new Secondary Approval Controls tab appears. This is where you manage your approval rules.

5. Click Add to open the Secondary Approval Wizard.

**Note:** One or more hosts must be configured in the HTA before a Secondary Approval control can be defined.

6. Select the group(s) for which this Secondary Approval control applies. These are the groups who will require additional approval to perform the vSphere Client operation. Only AD groups which are mapped to an HTA role (via rules) will appear in the list.

7. Click Next.

8. Select the resources (virtual machines and their folders) to which this Secondary Approval rule applies.

---

**Figure 6-2 Secondary Approval Wizard - Select Requestor Groups page**

**Figure 6-3 Secondary Approval Wizard - Select Resources page**
Secondary Approval
Configuring Secondary Approval

Note: Controls applied to virtual machine folder resources only propagate one level and therefore do not apply to resources in child folders. You must explicitly set controls for each individual folder if you wish to have the approval rule remain with it.

9. Click Next.

10. Select the vSphere operation(s) to which this Secondary Approval control applies.
11. Click Next.

12. Select the checkbox next to the AD groups whose users can approve the operations in this rule.
   Only AD groups associated with HTA roles that have the Secondary Approval/Approver privilege appear.

13. Enter the email address or email list where the HTA sends approval requests.
14. Click Next.
The Secondary Approval Wizard Control Summary page appears.

15. Verify the Secondary Approval control and click Finish.

The Secondary Approval Controls tab appears where you can see all currently defined approval rules.

Secondary Approval configuration is now complete. Anytime a user in the Requestor Group attempts to perform an operation that requires additional approval, a request is created and sent to the Approver Groups for approval.

Pending Requests

The Policy > Secondary Approval Requests page displays a list of all requests for which a user can approve or deny.

The following information is displayed for a given request:
Secondary Approval
Pending Requests

- Requestor—The user who initiated the request. Click on a Requestor to display the approve or deny request page.
- Resource—The resource the user was attempting to use.
- Operation—The operation the user was attempting to perform.
- Approver Groups—The user group who can approve or deny the request.
- Request Time—The date and time the request was initiated.
- Status—Shows the request is pending approval.

**Note:** Users will not see requests if they are not in the authorized approver group for the request which triggered the control.

**Approving**

Perform the following to approve a pending request:

1. Open the Secondary Approval Pending Request page in one of the following ways:
   - Click the link in the *Request for Secondary Approval* email notification you received and login.
   - Select **Policy > Secondary Approval Requests** in the HTA Management Console, select the checkbox next to the request, and click Approve.

![Secondary Approval Pending Request page](image)

*Figure 6-9  Secondary Approval Pending Request page*
2. Select the Approve option.

![Secondary Approval Pending Request - Approve page](image)

*Figure 6-10  Secondary Approval Pending Request - Approve page*

The following fields appear:

- **Start**—The date and time to allow the requested operation to start. Enter the date or click the calendar ( ) button and choose a date, and enter the time.
- **Duration (Hours)**—Specify how long, in hours, until the approval expires after the start time.
- **Email**—Enter the email address of the requestor.
- **Comments**—Enter any comments regarding this request.

3. Click Apply.

The requestor, approver, and approver group (if CC is enabled) will receive an email indicating the request was approved.

### Denying

Perform the following to deny a pending request:

1. Open the Secondary Approval Pending Request page in one of the following ways:
   - Click the link in the *Request for Secondary Approval* email notification you received and login.
Select **Policy > Secondary Approval Requests** in the HTA Management Console and select the checkbox next to the request and click Deny.

2. Select the Deny option.

The following fields appear:

- **Email**—Enter the email address of the requestor.
- **Comments**—Enter any comments regarding this request.

3. Click Apply.

The requestor, approver, and approver group (if CC is enabled) will receive an email indicating the request was denied.
Secondary Approval

Request History

The Policy > Secondary Approval Requests page History tab displays a history of all Secondary Approval requests.

<table>
<thead>
<tr>
<th>Requestor</th>
<th>Resource</th>
<th>Operation</th>
<th>Approver</th>
<th>Request Time</th>
<th>Approval/Denial Time</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>Virtual Center 10.235.36.11 &gt; Datacenter &gt; VirtualMachine: Payroll-VM</td>
<td>Remove from Inventory</td>
<td>superadmin</td>
<td>07/10/2012</td>
<td>07/10/2012</td>
<td>Approved</td>
</tr>
<tr>
<td>admin</td>
<td>Virtual Center 10.235.36.11 &gt; Datacenter &gt; VirtualMachine: Payroll-VM</td>
<td>Remove from Inventory</td>
<td>superadmin</td>
<td>07/10/2012</td>
<td>07/10/2012</td>
<td>Denied</td>
</tr>
<tr>
<td>back-up-admin</td>
<td>Virtual Center 10.235.36.11 &gt; Datacenter &gt; VirtualMachine: SalesRep-VM</td>
<td>Delete a Snapshot</td>
<td>superadmin</td>
<td>07/10/2012</td>
<td>07/10/2012</td>
<td>Approved</td>
</tr>
</tbody>
</table>

Figure 6-13  Policy > Secondary Approval Requests - History tab

The following information is displayed for a given request:

- Requestor—The user who initiated the request. Click on a Requestor to display the Secondary Approval Details page.
- Resource—The resource the user was attempting to use.
- Operation—The operation the user was attempting to perform.
- Approver—The user who approved or denied the request.
- Request Time—The date and time the request was initiated.
- Approval/Denial Time—The date and time the request was approved or denied.
- Status—Shows whether the request was approved or denied.

Figure 6-14  Secondary Approval Request Details page
CHAPTER 7

Logging

This chapter contains the following sections:

- Logging Overview
- Configuring Syslog Settings
- Viewing HTA Log Messages
- Obtaining Troubleshooting Bundle
- Obtaining System Logs

Logging Overview

Logs provide a record of the events occurring within the virtual infrastructure. The HTA logs are useful for performing auditing, forensic analysis, supporting internal investigations, establishing baselines, and identifying operational trends and long-term problems pertaining to the virtual infrastructure security, compliance monitoring, and enforcement.

Individual log entries contain information related to a specific event that has occurred within a system or network. Routine log analysis is beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems.

Log messages generally contain a date and timestamp, hostname, priority, a message ID, and additional information describing who performed (or tried to perform) an action, from what location, to what target object.

HTA log messages have the following format:

Date: Host: Priority: Message ID: Message

Logs retrieved from a vCenter Server have the following format:

Date(posted): Date(event) VC: Host: Message (as logged by vCenter)

Note: By default, vCenter Server events are not sent to the HTA. You can enable the Get vCenter events scheduled event from the Compliance > Scheduled Events page to update the HTA log with events from all protected vCenter Servers—see Scheduling Events on page 49.

While the HTA has a comprehensive view of all user initiated vSphere operations in the
virtual infrastructure, importing vCenter Server events may be useful for completeness and to include automated events such as DRS.

Refer to Syslog Severity Level Classifications on page 98 for details on the five log level classifications.

All local log files generated on the HTA host are stored in the /var/log/asc directory, even if the HTA is configured to export logs to an external Syslog server. Log files are rotated when they reach their maximum allotted size.

### Configuring Syslog Settings

The HTA logs all operations initiated on its vCenter Server or ESX hosts, for all methods of access, and stores the corresponding log entries in a central location.

**Note:** Optionally, you can have the HTA automatically retrieve the vCenter Server events and have them included in the HTA log files. (Enable the predefined Get vCenter events scheduled event to activate vCenter Server event retrieval—see Scheduling Events on page 49.)

Log entries are human readable and include information on the user initiating the operation, user group affiliation, origin (method of access and source), object being manipulated, the operation itself, and whether the operation was authorized. The HTA provides detailed logs to support easy audit and compliance reporting, and log file export.

### Syslog Severity Level Classifications

Individual log entries are classified by importance. For example, all successful operations are classified as INFO level log entries. Events that have security implications such as failed authorization, are logged with WARN level.

There are five log level classifications:

- **FATAL**—Severe errors, usually involving a crash.
- **ERROR**—Runtime errors, intermittent network issues, recoverable errors such as dropping network packets, etc.
- **WARN**—Non-fatal, unexpected behavior, and proactive monitoring notifications. Security events, such as failed authorizations, are also logged at this level.
- **INFO**—Generally interesting events, such as virtual machine moves and configuration changes. Also includes all virtual infrastructure events, including successful and failed authentications, authorizations, and changes to virtual infrastructure configurations that were locked down by the HTA.
- **DEBUG**—Support messages about the internal operations of the HTA that are intended for use by HyTrust Support.

You can view Syslog events using the built-in log viewer (General > Log Viewer).

### Appliance and Host Logging

By default, the HTA stores aggregated Syslog files locally. However, you can configure the HTA to send its logs to an external Syslog server, which you can specify by IP address. All
local HTA log files are stored in the \texttt{/var/log/asc} directory. The \texttt{/var/log} directory is configured as a separate virtual disk per CIS benchmark recommendations for ESX hosts. Log files are rotated when they reach their maximum allotted size. Note that if you set the log level to include debug messages, the logs and log rate increases significantly.

\textbf{Note:} If you need to configure multiple Syslog servers use the HTA Command Line Interface—see Appendix G, HTA Command Line Interface.

The HTA-specific logs may be downloaded, purged, or re-indexed. Use re-indexing if you are experiencing trouble viewing the logs in the log viewer (\texttt{General > Log Viewer}) page. Similarly, for HTA-protected ESX hosts you can specify options to store logs on the host (local), or you can choose to send the logs to an explicit Syslog server. The default is to log messages in a file stored locally on each host.

You may explicitly set up individual host logging locations and set individual host logging options when you initially add a host to be protected by the HTA (use the Advanced tab on the Add Host page). You can also go back later to select a host from the Edit Host page (\texttt{Compliance > Hosts}) and modify its current logging location.

\textbf{Note:} The Syslog Server setting on the Advanced tab of the Add/Edit Host page will override the Syslog Server setting under the Host Default Logging Configuration section on the \texttt{Configuration > Logging} page.

You can use the \texttt{remote_syslogd} operation in a template (\texttt{Compliance > Templates}) to setup logging to a remote logging server. To learn more about deploying security templates, see Host Configuration Templates on page 70.

To specify the HTA and ESX Host default logging configurations:
1. Select **Configuration > Logging** from the HTA Management Console.

![Logging Configuration](image)

**Figure 7-1**  **Configuration > Logging page**

2. On this page you can configure logging levels, the location for the HTA to aggregate Syslog files, and default logging aggregation locations for hosts.

For details on the Logging Configuration page settings see the **Appliance Configuration Options** on page 100 and **ESX and ESXi Host Configuration Options** on page 101.

**Appliance Configuration Options**

The following fields are available in the *HTA Logging Configuration* section on the Logging Configuration (**Configuration > Logging**) page (see **Figure 7-1**):

- **Logging Level**—Set the level of logging to capture. Levels are FATAL, ERROR, WARN, INFO, and DEBUG—see **Syslog Severity Level Classifications** on page 98.
- **HTA Logging Aggregation**—Specify whether the HTA aggregated Syslog files are stored locally (the default) or sent to an external Syslog server.

The following fields are available for external Syslog servers:

- **HTA Logging Aggregation Template Type**—The logging format type (HyTrust Proprietary or CEF).
- **HTA Syslog Servers**—A comma-separated list of external Syslog server IP addresses.
- **Encrypt Syslog**—Enable (selected) or disable (deselected) encryption for messages sent to the external Syslog server.
Manage Logs—Click the Download button to download the HTA log files.

Log Viewer—Click the Reset button to delete the existing log viewer index and reset (clear) the entries in the log viewer. The log files themselves are not deleted.

**ESX and ESXi Host Configuration Options**

The following fields are available in the Host Default Logging Configuration section on the Logging Configuration (Configuration > Logging) page (see Figure 7-1):

- Default Logging Aggregation—Specify whether HTA-protected hosts store log files locally (the default) or send them to an external Syslog server.

  The following field is available for external Syslog servers:

  - Default Syslog Server—The IP address of the external Syslog server. This field is only available if hosts send log files to an external Syslog server.

**Viewing HTA Log Messages**

You can view HTA log messages from either the HTA Management Console or the command line interface (CLI).

**From the Management Console**

Open the **General > Log Viewer** page to view the HTA log messages from the HTA Management Console.

![Log Viewer](image)

**Figure 7-2 General > Log Viewer page**
Logging
Viewing HTA Log Messages

The HTA Management Console Log Viewer is split into two sections. The top section summarizes the log entry and includes the following information:

- Date
- Priority
- User
- Operation
- Resource Name
- Resource Type
- Status

The bottom section displays the full log message information for the selected log entry.

You can use the search field to help locate a particular log message. You can filter by log priority using the Fatal, Error, Warn, and Info checkboxes.

Selecting the Message Column checkbox adds a new column to the top summary section which displays additional information about the log entry.

Click a log entry date (in the first column) to display its message details in the lower section of the page. Click the triangle to the left of Message Detail to display additional message information.

Other logs, such as proxy-ssh.log, htcli.log, and asc.debug, are viewable from the HTA CLI.

Log Message Information

HTA Management Console log messages may contain the following information:

- Date—The date the entry was generated.
- User—The user performing the operation that generated the entry.
- Groups—The user's group name.
- Operation—The operation.
- Resource Name—The resource where the operation is being performed.
- Resource Type—The resource type (e.g., VM, HOST, CONSOLE).
- Privileges—The privileges required to perform the requested operation.
- Rules—The rule(s) in effect for the resource to which the operation applies.
- Parameters—The operation parameters.
- Message ID—The HTA specific log message identifier.
- Priority—The log entry's classification level (FATAL, ERROR, WARN, INFO, or DEBUG).
- Source—The host where the user attempted the operation.
- Destination—The target host/object for the operation.
- Status—Indicates whether the requested operation was permitted or denied.
From the CLI

You can view HTA log messages in their entirety from the command line interface (CLI) using the `asc log` command—see Appendix G, HTA Command Line Interface.

An example log message from the `proxy-ssh.log` file looks as follows:

```
Mar 16 16:35:38 localhost proxy-ssh[7066]: [root@172.16.1.200]@[172.16.1.22] Authenticating user
```

The `proxy-ssh.log` shows all SSH connection messages. Each message includes details about who tried to do what from where.

### Obtaining Troubleshooting Bundle

This section describes how to obtain the HTA troubleshooting bundle to send to HyTrust Support.

To obtain the HTA troubleshooting bundle:

1. Login via SSH to the HTA using the `ascadminuser` credentials.
2. Enter the following command:
   ```
   asc log -t
   ```
   This command generates a troubleshooting archive zip file (`asc-state.zip`) and saves it in the `/var/log/asc` directory—see `asc log` on page 142.
   
3. Once the zip file has been created, use secure copy (SCP) to move the file to a local client machine and then contact HyTrust Support for further assistance.

### Obtaining System Logs

This section describes how to obtain the HTA system log file(s).

To obtain the HTA system logs:
1. Open the **Configuration > Logging** page.

![Configuration > Logging page](image)

**Figure 7-4 Configuration > Logging page**

2. Click the Download button and save the archive (asc.log.zip).
Monitoring Hosts and Networks

This chapter contains the following sections:

- Enabling Monitoring
- Network Resource Monitoring
- Protected Host Monitoring
- NRM and PHM Status
- Enable/Disable NRM
- Enable/Disable PHM
- SNMP Alerts and SMTP Notifications

Enabling Monitoring

The HTA can perform ICMP ping tests and port scanning for its dependent network infrastructure and protected resources, as well as send notifications. Access to this feature is available through the HTA CLI using the `asc monitor` command—see Appendix G, HTA Command Line Interface.

To enable SNMP monitoring via the HTA CLI, type:

```
asc monitor -n on
```

To enable SNMP monitoring via the HTA Management Console, refer to Configuring Notifications on page 52.

Monitoring becomes enabled by default if the vCenter Server and any corresponding hosts are protected by the HTA.

Network Resource Monitoring

The HTA scans all routers, time servers, name servers, log servers, SNMP trap receivers, SMTP servers, and Active Directory/LDAP service ports during its health monitoring routine, which runs at 2 minute intervals (via a `cron` job). This is called network resource monitoring.
Monitoring Hosts and Networks

Protected Host Monitoring

The HTA uses the `monit` service to perform ICMP ping tests to all protected vCenter Servers and ESX/ESXi hosts. This is called protected host monitoring (PHM). All failures are listed under the Resources section in the Appliance Dashboard—see Appliance Dashboard on page 17.

In the HTA CLI, an offline ESX or ESXi host state will show `Warning`, and an offline protected vCenter Server will show `Failed`.

NRM and PHM Status

You can view NRM and PHM status on the Appliance Dashboard or via the CLI.

Appliance Dashboard

The Appliance Dashboard shows both NRM and PHM warnings and errors. For example, in the figure below DNS (NRM) shows as `OK` and Protected Host Monitoring (PHM) shows as `Disabled`.

![HTA Dashboard with NRM and PHM status](image)

Figure 8-1   HTA Dashboard with NRM and PHM status
Appliance Command Line Interface

Using the local HTA administrator account (ascadminuser), you can view NRM and PHM errors and warnings via the CLI using the asc monitor command. To learn more about this command, type:

```bash
asc monitor --help
```

To view the health of the HTA configuration, services, and resources, type:

```bash
asc monitor --status
```

In the figure below, the DNS (NRM) shows as Healthy/OK and the PHM shows as Disabled.

![Figure 8-2 HTA CLI with NRM and PHM status](image)

Enable/Disable NRM

**Note:** NRM is enabled by default.

To enable network resource monitoring, type:

```bash
asc monitor --network on
```

The Monitor Network Services configuration in the HTA CLI will now show an Enabled value of True.

To disable network resource monitoring, type:
Enable/Disable PHM

Note: PHM is disabled by default.

To enable protected host monitoring, type:

```
asc monitor --protected on
```

The Monitor Protected Hosts configuration in the HTA CLI will now show an Enabled value of True.

To disable protected host monitoring, type:

```
asc monitor --protected off
```

The Monitor Protected Hosts configuration in the HTA CLI will now show an Enabled value of False.

Refer to Appendix G, HTA Command Line Interface for more details on this command.

SNMP Alerts and SMTP Notifications

SNMP alerts are generated when a service or resource transitions between Ok, Warning, and Failed and are distributed via SNMP, SMTP, or Syslog. A PHM connectivity issue to a vCenter Server is a Failed state, and a connectivity issue to a Nexus 1000V VSM, ESX, and ESXi is a Warning state.

Use the `asc monitor` command to configure SNMP alerts using the HTA CLI, and refer to the examples in the help text. Refer to Appendix G, HTA Command Line Interface for more details on this command.

You can also use the HTA Management Console to configure SNMP alerts and SMTP notifications—see Configuring Notifications on page 52.
Maintaining the Appliance

This chapter contains the following sections:

- Licenses
- Services
- Troubleshooting
- Jobs
- Searches

Licenses

An HTA administrator can view the current license the HTA is using on the Maintenance > License page.

![License Page Screenshot](image)

**Figure 9-1** Maintenance > License page
The License page contains details such as the maximum number of protected hosts, maintenance expiration date, and support expiration date. Details vary depending on license type.

Additional licenses, including maintenance and support renewals, may be obtained by contacting sales@hytrust.com.

To install a new license, use the Upgrade tab on the Maintenance > License page or use the HTA CLI `asc upgrade -i` command.

![Figure 9-2 Maintenance > License - Upgrade tab](image)

### Services

The Maintenance > Services page provides an easy to use interface to enable or disable services running on the HTA.

![Figure 9-3 Maintenance > Services page](image)

You can restart the HTA HTTP/SOAP proxy. (You will need to re-login to the HTA Management Console if you restart the HTTP/SOAP proxy.)

The SSH proxy service status is displayed above the Start/Stop button.
The default Proxy Denial Message is *Permission denied by HyTrust Appliance*. This message is presented to any user that attempts to perform an operation that goes beyond their privilege level in both SSH and the vSphere Client. An HTA administrator can also customize the denial message.

Click the ReIndex button if you are having trouble searching for rules or resources that should be present or if you are seeing unexpected duplicates.

**Troubleshooting**

The [Maintenance > Troubleshooting](#) page allows an HTA administrator to reboot the HTA system.

![Figure 9-4 Maintenance > Troubleshooting page](#)

Click the Reboot button to reboot the HTA system.
The Maintenance > Jobs page allows an HTA administrator to view completed jobs, see running jobs, and also kill jobs.

### The Maintenance > Jobs Page

**Figure 9-5 Maintenance > Jobs page**

The information displayed for a given job include the following:

- **Kill**—Click the Kill Service ( zwłon) icon to manually kill a job that is in the Running state.
- **Service**—The service type.
- **Started**—The date and time when the job started.
- **Ended**—The date and time when the job ended.
- **User**—The name of the user account that initiated the job.
- **Host**—The host which initiated the job.
- **Template**—The template (or operation) used for the job.
- **Status**—The status of the job.

### Searches

The HTA supports searching vCenter Server resources from the General > Search page when assigning Rules, RuleSets, or Labels to policy resources and when assigning rules to
RuleSets. You can also narrow your searches using filters to locate a particular object such as a Host, Virtual Machine, or vSwitch.

As shown in Figure 9-6, only the Virtual Center, Host, and Virtual Machine filters were selected. Clicking a link in the search results (e.g., SJ-VM-1) displays details about the selected object in the right pane. You can also hover the mouse cursor over an item in the search results to view its resource tree path (and other details such as the virtual center and data center) as shown in the figure below.

For details about the fields within the HTA that are indexed or to see some sample queries using the search field, click on the help ( ) icon or refer to Appendix E, Search Filters.

Searching is also supported in the Log Viewer—see Viewing HTA Log Messages on page 101.

The HTA utilizes the Apache Lucene™ full-featured text search engine library. The HTA indexes are updated any time information about an HTA object is added, removed, or
updated. For additional information regarding Lucene, refer to http://lucene.apache.org/java/3_1_0/queryparsersyntax.html.
# Default Appliance Roles and Permissions

## Table A-1  Default Roles and Permissions

<table>
<thead>
<tr>
<th>Group Name (AD)</th>
<th>HTA Role</th>
<th>DEMO</th>
<th>Description</th>
</tr>
</thead>
</table>
| HT_ApplAdmin      | HTA Administrator (ASC_ApplAdmin)              | Yes  | Install the HTA and perform configuration tasks:  
  - Configure networking  
  - Configure high availability  
  - Configure logging  
  No privileges to manipulate the virtual infrastructure. |
<p>| HT_ARCAdmin       | ARC Administrator (ASC_ARCAdmin)               | Yes  | Create and modify ARC templates, add ARC targets, assess ARC, and remediate ARC.                                                              |
| HT_ARCAssessor    | ARC Assessor (ASC_ARCAssessor)                 | Yes  | Perform ARC assessments and view ARC results.                                                                                                  |
| HT_BackupAdmin    | Backup Administrator (ASC_BackupAdmin)         | Yes  | Backup and restore virtual machines (guests).                                                                                                  |
| HT_BASICLogin     | Basic Login (ASC_BASICLogin)                  | Yes  | Perform some basic operations like login.                                                                                                      |
| HT_CoreApplAdmin  | Core Appliance Administrator (ASC_CoreApplAdmin)| Yes  | Install and configure core appliance virtual machines.                                                                                         |
| HT_DCAdmin        | Datacenter Administrator (ASC_DCAdmin)        | Yes  | Set up VMware vCenter Server data centers and perform actions on all objects within virtual data centers.                                      |</p>
<table>
<thead>
<tr>
<th>Group Name (AD)</th>
<th>HTA Role</th>
<th>DEMO</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HT_ESXMAadmin</td>
<td>ESX Maintenance Administrator (ASC_ESXMAadmin)</td>
<td>Yes</td>
<td>Install patches, change ESX host configurations, and reboot ESX hosts.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Perform ESX/ESXi host maintenance (use SSH, change configuration, reboot). Perform HTA configuration,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>assessment, and remediation (ARC). No virtual machine privileges.</td>
</tr>
<tr>
<td>HT_NetworkAdmin</td>
<td>Network Administrator (ASC_NetworkAdmin)</td>
<td>Yes</td>
<td>Manage virtual switches, VLANs, and other network configuration settings.</td>
</tr>
<tr>
<td>HT_PolicyAdmin</td>
<td>Policy Administrator (ASC_PolicyAdmin)</td>
<td>Yes</td>
<td>Create and modify policies, labels, and constraints.</td>
</tr>
<tr>
<td>HT_RoleAdmin</td>
<td>Role Administrator (ASC_RoleAdmin)</td>
<td>Yes</td>
<td>Create and modify roles and privileges.</td>
</tr>
<tr>
<td>HT_StorageAdmin</td>
<td>Storage Administrator (ASC_StorageAdmin)</td>
<td>Yes</td>
<td>Define VMFS volumes and mapping to LUNs including masking and zoning. Privileges also include:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Define iSCSI access paths.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Manage NFS volumes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Manage HSM and data retention.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Administer storage (disk replacement).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Manage backup.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Manage datastores and datastore clusters.</td>
</tr>
<tr>
<td>HT_SuperAdmin</td>
<td>Super-user Administrator (ASC_SuperAdmin)</td>
<td>Yes</td>
<td>Perform any action. (Assigned all privileges).</td>
</tr>
<tr>
<td>HT_UCSLogin</td>
<td>Cisco UCS Login (ASC_UCSLogin)</td>
<td>Yes</td>
<td>Access and perform operations with Cisco UCS Manager.</td>
</tr>
<tr>
<td>HT_VIAdmin</td>
<td>Virtual Infrastructure Administrator (ASC_VIAdmin)</td>
<td>Yes</td>
<td>Perform virtual infrastructure operations. Configure DRS and VMware HA. Initiate VMotion. Assign</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>hosts to resource pools.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Limited privileges on ESX hosts.</td>
</tr>
<tr>
<td>Group Name (AD)</td>
<td>HTA Role</td>
<td>DEMO</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------</td>
<td>------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| HT_VMPowerUser  | Virtual Machine Power User (ASC_VMPowerUser) | Yes | Perform actions on virtual machines and resource objects. Role members may view and change most virtual machine configuration settings, take snapshots, and schedule tasks. Privileges include:  
- All privileges for scheduled task privileges group.  
- Selected privileges for global items, datastore, and virtual machine privileges groups.  
No privileges for folder, datacenter, network, host, resource, alarms, sessions, performance, and permissions privileges groups. |
| HT_VMUser       | Virtual Machine User (ASC_VMUser) | Yes | This role is equivalent to the role with the same name defined in vCenter Server 1.x. Role members may interact with virtual machines, but not change the virtual machine configuration. Privileges include:  
- All privileges for the scheduled tasks privileges group.  
- Selected privileges for the global items and virtual machine privileges groups.  
No privileges for the folder, data center, datastore, network, host, resource, alarms, sessions, performance, and permissions privileges groups. |
Appendix B

Summary of All HTA Management Console Operations

The following table shows the various menu options available in the HTA Management Console.

Note: These items are available to users based on permissions assigned to the corresponding Demo or AD groups.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Dashboard</td>
<td>Displays a summary of HTA information such as Hostname, IP address(es), services, license info, and resources.</td>
</tr>
<tr>
<td></td>
<td>Log Viewer</td>
<td>A built-in HTA log viewer.</td>
</tr>
<tr>
<td></td>
<td>Search</td>
<td>Search the virtual infrastructure resources.</td>
</tr>
<tr>
<td>Menu</td>
<td>Page</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Compliance</td>
<td>Hosts</td>
<td>Lists all discovered and manually configured ESX hosts, vCenter Servers, and Cisco Nexus 1000V and display their status based on HTA monitoring.</td>
</tr>
<tr>
<td></td>
<td>History</td>
<td>View compliance history.</td>
</tr>
<tr>
<td></td>
<td>Templates</td>
<td>Lists all templates (built-in and custom) that may be used to assess and enforce compliance on specific protected ESX hosts.</td>
</tr>
<tr>
<td></td>
<td>Scheduled Events</td>
<td>Lists all scheduled assessments, which you can view or delete.</td>
</tr>
<tr>
<td>Policy</td>
<td>Resources</td>
<td>Shows all resources for a given policy.</td>
</tr>
<tr>
<td></td>
<td>Rules</td>
<td>View and manage HTA rules. Rules are triples of domain user groups, roles, and constraints.</td>
</tr>
<tr>
<td></td>
<td>Roles</td>
<td>View and manage HTA roles. Roles are collections of privileges or permissions that let an administrator group together operations, usually defined along the same lines as roles or duties that users perform within an organization.</td>
</tr>
<tr>
<td></td>
<td>RuleSets</td>
<td>View and manage HTA RuleSets. RuleSets provide a way to assign policy based on the class of the virtual infrastructure objects rather than their location in the hierarchy.</td>
</tr>
<tr>
<td></td>
<td>Labels</td>
<td>View and manage HTA labels. Labels are used to classify or categorize policy resources.</td>
</tr>
<tr>
<td></td>
<td>History</td>
<td>Lists all active, draft, and archived policies, including policies automatically imported when a vCenter Server is added to the HTA.</td>
</tr>
<tr>
<td></td>
<td>Secondary Approval Requests</td>
<td>View and manage Secondary Approval requests.</td>
</tr>
</tbody>
</table>
### Table B-1  HTA Management Console Operations Summary (Continued)

<table>
<thead>
<tr>
<th>Menu</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td>Network</td>
<td>View and manage IP addresses, ports, and other HTA network configuration settings.</td>
</tr>
<tr>
<td></td>
<td>Static Routes</td>
<td>View and manage HTA static routes.</td>
</tr>
<tr>
<td></td>
<td>Authentication</td>
<td>Specify authentication mode and set connection settings to use Active Directory for HTA role-based authentication and authorization.</td>
</tr>
<tr>
<td></td>
<td>Secondary Approval</td>
<td>Enable Secondary Approval and configure notification settings.</td>
</tr>
<tr>
<td></td>
<td>Two-Factor</td>
<td>Enable RSA SecurID and upload an RSA SecurID configuration file, or enable and configure CA AuthMinder.</td>
</tr>
<tr>
<td></td>
<td>Certificates</td>
<td>View, generate, and install SSL certificates for the Web Application or Logging services.</td>
</tr>
<tr>
<td></td>
<td>Logging</td>
<td>Configure HTA and ESX host logging options and settings.</td>
</tr>
<tr>
<td></td>
<td>Monitoring</td>
<td>Configure monitoring functions such as SNMP and SMTP notifications.</td>
</tr>
<tr>
<td></td>
<td>vCenter Plugin</td>
<td>Configure the vCenter Plugin to allow access to the HTA Management Console from a vCenter Server.</td>
</tr>
<tr>
<td></td>
<td>Root Password Vaulting</td>
<td>Manage recovery passcodes for hypervisor root passwords.</td>
</tr>
<tr>
<td></td>
<td>Password Requirements</td>
<td>Configure password complexity for the local ascadminuser administrator account.</td>
</tr>
<tr>
<td></td>
<td>Trusted Execution</td>
<td>Setup Intel TXT (trust) between the hardware and the VMware vSphere infrastructure.</td>
</tr>
<tr>
<td></td>
<td>Third Party Configuration</td>
<td>Integrate the HTA with a third party product, such as Trend Micro Deep Security Manager or CA Virtual Assurance for Infrastructure Manager.</td>
</tr>
<tr>
<td>Maintenance</td>
<td>License</td>
<td>View a summary of the registered HTA license or install a new license.</td>
</tr>
<tr>
<td></td>
<td>Services</td>
<td>View the SSH proxy status, start and stop the SSH proxy, restart the HTTP/SOAP proxy, change the proxy denial message, or reindex the policy.</td>
</tr>
<tr>
<td></td>
<td>Troubleshooting</td>
<td>Reboot the HTA.</td>
</tr>
<tr>
<td></td>
<td>Jobs</td>
<td>View completed jobs, jobs that are running, and also kill jobs.</td>
</tr>
</tbody>
</table>
## HTA Management Console Operations Summary (Continued)

<table>
<thead>
<tr>
<th>Menu</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Help</td>
<td>Support</td>
<td>Display HyTrust Support information and links.</td>
</tr>
<tr>
<td></td>
<td>Installation Guide</td>
<td>Open the <em>HyTrust Appliance Installation Guide</em>.</td>
</tr>
<tr>
<td></td>
<td>Administration Guide</td>
<td>Open the <em>HyTrust Appliance Administration Guide</em> (this document).</td>
</tr>
</tbody>
</table>
Root Password Recovery

This appendix contains the following sections:

- Recovering From the HTA
- Recovering From A Client System

For the purpose of emergency recovery, ESX host root passwords are encrypted with a strong key derived from the user provided passcode and forwarded to the Syslog server for inclusion in the asc.log file.

In the rare case where the HTA is not available, but privileged maintenance access to ESX servers is required, the passwords can be recovered from either the HTA or a client system.

Recovering From the HTA

Perform the following to recover a root password from the HTA:

1. Deploy a new HTA (using the OVF file). The new HTA must be the same version and build number as the HTA that failed.
2. Power On the new HTA and login as ascadminuser with the password Pa$$w0rd123!.
3. Assign new credentials to the local HTA administrator account (ascadminuser)—see Changing the ascadminuser Password on page 58.
4. Obtain the passcode that was assigned when Root Password Vaulting was initially configured in the HTA.
5. Obtain a copy of the HTA logs with the last 5 days of events.
6. Locate the following line in the logs for each host where the password needs to be recovered (addresses and hashes will vary between hosts):
   
   Update root account: host <IP address> to <32-bit hash A> - <32-bit hash B>

7. Enter the following command to recover the root password:
   
   recoverpassword -k <passcode> -u <32-bit hash A> -p <32-bit hash B>

   Where:
   
   - <32-bit hash A> — is the encrypted username.
   - <32-bit hash B> — is the encrypted password.
Recovering From A Client System

Perform the following to recover a root password from a client system:

1. If Connection 1 (eth0) of the HTA is accessible via SSH, another option is to secure copy (SCP) the RecoverPassword-1.0.zip file to a 32-bit Windows environment and run the RecoverPassword-1.0.jar file on your client machine.

   Note: The RecoverPassword-1.0.zip file is in the ~/tools/rpv directory.

2. Download and install the Java Runtime Environment (JRE) on your client machine. The JRE download can be found at: http://java.com/en/download/index.jsp.

3. Obtain the passcode that was assigned when Root Password Vaulting was initially configured in the HTA.

4. Obtain a copy of the HTA logs with the last 5 days of events.

5. Locate the following line in the logs for each host where the password needs to be recovered (addresses and hashes will vary between hosts):
   
   Update root account: host <IP address> to <32-bit hash A> - <32-bit hash B>

6. On your Windows machine run the following command:

   <full path>\java.exe -jar <full path>\RecoverPassword.jar -k <passcode> -u <32-bit hash A> -p <32-bit hash B>

Another alternative would be to assign an eth0 IP address to the HTA using the setup command. Once Connection 1 has been configured, you can open an SSH session to the HTA and run the recoverpassword command as shown above.
Protecting ESX/ESXi Hypervisors

This appendix contains the following sections:

- Mapped Mode
- Router Mode

**Mapped Mode**

The following is required to protect the ESX or ESXi hypervisor hosting the HTA virtual appliance in Mapped Mode:

- **ESX:**
  - No special wiring is required as long as the HTA can talk to the ESX Service Console.
  - On the Add/Edit Host page, be sure to select the **HTA** checkbox in the General tab and the **Lock Out Unauthorized Access** checkbox in the Advanced tab for the associated ESX host.

- **ESXi:**
  - No special wiring is required as long as the HTA can talk to the ESXi VMkernel port.
  - The HTA must be licensed for Root Password Vaulting (Enterprise or appropriate evaluation license).
  - On the Add/Edit Host page, be sure to select the **HTA** checkbox and the **Root Password Vaulting** checkbox in the General tab for the associated ESXi host running the HTA virtual machine.

**Router Mode**

The example in this section is only one connectivity example. Other implementations are possible and can be varied for different network environments. However, the sole access path to the ESX Service Console (or VMkernel Port, in the case of ESXi) must be through the HTA (i.e., if either HTA network interface is disconnected the management clients are unable to ping the ESX/ESXi Service Console IP address).
The following is an example of how to protect an ESX or ESXi hypervisor hosting the HTA virtual appliance in Router Mode:

**Note:**
All ESX/ESXi Service Consoles and vCenter Servers must reside on different subnets from the VMware management clients before the information below can be followed.

1. Locate the vSwitch where the Service Console Port is located.
2. On the same vSwitch as the Service Console:
   a. Create a port group called `NetworkAdminProtected` on the ESX/ESXi host. This port group will share the same protected network subnet as the Service Console (and VLAN ID if enabled).
   b. Create a second port group called `NetworkAdmin` on the ESX/ESXi host. This port group will be assigned to the client management subnet (and VLAN ID if enabled).

3. Add a temporary Windows System (VM Client) to the `NetworkAdminProtected` network.
4. From the VM Client, open the vSphere Client and connect to the ESX host where you want to install the HTA.
5. Deploy the HTA using the OVF file.
6. Assign the HTA Connection 1 interface to the `NetworkAdmin` port group.
7. Assign the HTA Connection 2 interface to the `NetworkAdminProtected` port group.
8. Boot the HTA and assign the Connection 1 interface an IP address on the client management subnet.

**Note:** The Connection 1 IP address is to be used as a route destination by hosts (or another router) on the client management subnet.

9. From a web browser on a client machine connected to the client management subnet, enter the URL location of the HTA virtual machine, for example: `https://172.16.2.110/asc`
10. Enter the login username and password of an HTA user at your site. (If you are still in Demo mode, login as `superadminuser` with the password `Pa$$w0rd123!`.)
11. In the HTA setup wizard, select Router Mode and assign the Connection 2 interface an IP address on the `NetworkAdminProtected` subnet.
12. On the General tab of the Add Host (or Edit Host) page:
   a. Add the HTA host.
   b. Specify the IP address (on the Service Console subnet).
   c. Add the root credentials of the local ESX/ESXi.
   d. Select the HTA checkbox.

13. Open the vSphere Client and connect to the ESX/ESXi Service Console from the client management subnet (NetworkAdmin) using an HTA user (e.g., superadminuser).

14. Remove the temporary VM Client from the protected network (NetworkAdminProtected).

![Figure D-2 HTA host in Router Mode](image)
Router Mode
Search Filters

The HTA allows you to search for the following policy resource attributes:

- Description
- FQDN
- Friendly Name
- IP Address
- Label
- Patch Level
- Published IP Address
- Resource Type
- RuleSet
- Template Type
- Trust Status

You can refine your searches using the following wildcard characters:

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>Replace a single character.</td>
</tr>
<tr>
<td>*</td>
<td>Replace one or more characters.</td>
</tr>
</tbody>
</table>

**Note:** You cannot use a * or ? as the first character of a search.

To search for multiple words, enclose the words with quotation marks.

The HTA Management Console Search page (General > Search) contains filters, in the form of checkboxes, to help you narrow down the search results to certain resource types in a typical network.
Below is the list of available filters.

**Table E-2  Search Filters**

<table>
<thead>
<tr>
<th>Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster</td>
</tr>
<tr>
<td>DataCenter</td>
</tr>
<tr>
<td>datastore</td>
</tr>
<tr>
<td>Folder</td>
</tr>
<tr>
<td>Host</td>
</tr>
<tr>
<td>Network</td>
</tr>
<tr>
<td>Portgroup</td>
</tr>
<tr>
<td>Resource Pool</td>
</tr>
<tr>
<td>Show Archived Versions</td>
</tr>
<tr>
<td>Virtual Application</td>
</tr>
<tr>
<td>Virtual Center</td>
</tr>
<tr>
<td>Virtual Machine</td>
</tr>
<tr>
<td>vSwitch</td>
</tr>
</tbody>
</table>

**Note:** The Show Archived Versions filter extends the search to older policies that have been archived. These policies are hidden from normal search results.
This appendix describes how the HyTrust Appliance (HTA) works in conjunction with the Cisco Nexus 1000V Software Switch.

The Cisco Nexus 1000V Series switches provide consistent, policy-based network and security services for a connected virtual infrastructure, in roughly the same way that Cisco administrators perform network management with a physical infrastructure. Using the Cisco NX-OS software platform, a network administrator can administer all the network interfaces of every attached VMware ESX or ESXi host as a single network switch and configure all the virtual network properties of an entire virtual infrastructure from a single Cisco IOS interface.

Providing protection for a virtual infrastructure and the virtual machines connected via a Nexus 1000V VSM is essentially the same as adding a vCenter Server instance and its managed hosts to the HTA environment. Once added, you can apply rules and assign roles in the same way as you currently do for vCenter Server instances and their managed ESX or ESXi hosts.

For Cisco Nexus 1000V switches, the HTA also provides additional privileges to define policies and control access to Nexus 1000V switches and any virtual infrastructures, hosts, and virtual machines attached or connected to the switch.

The following table lists the three HTA privileges that specify control of Cisco Nexus 1000V operations.

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NxOsConfig</td>
<td>Controls access and use of all other commands directed to the Cisco Nexus 1000V switches.</td>
</tr>
<tr>
<td>NxOsShow</td>
<td>Controls access to highly-restricted read-only sessions with Cisco Nexus 1000V switches.</td>
</tr>
<tr>
<td>NxOsXmlApi</td>
<td>Controls use of the interactive XML interface with Cisco Nexus 1000V switches.</td>
</tr>
</tbody>
</table>
The privileges listed in Table F-1 control access to the Cisco Nexus 1000V and are included in the predefined ASC_SuperAdmin and ASC_NetworkAdmin roles.

To view these privileges:

1. Open the Policy > Roles page.

2. Select the ASC_SuperAdmin role. (You may have to scroll the next page to see it.)

3. Expand the Privileges and HTA sections of the hierarchy to locate NxOsConfig, NxOsShow, and NxOsXmlApi.
There are several commands available via the HTA Command Line Interface (CLI). You access the HTA CLI from the vSphere Client Console tab, the vCenter Server Console, or an SSH session using the ascadminuser account.

**Note:** You can type asc at anytime to view the available HTA CLI commands.

To learn more about each command, type the name (e.g. asc backup) to get a description of the command and its intended usage. Include the -h or --help option for detailed syntax usage (e.g. asc backup --help).

The table below lists the commands available in the HTA CLI.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>asc auth</td>
<td>Test user authentication and authorization.</td>
</tr>
<tr>
<td>asc backup</td>
<td>Manage configuration backup and restore.</td>
</tr>
<tr>
<td>asc certs</td>
<td>Manage x509 certificates.</td>
</tr>
<tr>
<td>asc firewall</td>
<td>Manage the forwarding firewall.</td>
</tr>
<tr>
<td>asc ha</td>
<td>Manage OS and application-level high availability (HA).</td>
</tr>
<tr>
<td>asc log</td>
<td>Manage system logging.</td>
</tr>
<tr>
<td>asc monitor</td>
<td>Manage monitoring interfaces.</td>
</tr>
<tr>
<td>asc network</td>
<td>Manage network resources.</td>
</tr>
<tr>
<td>asc policy</td>
<td>Manage policies.</td>
</tr>
<tr>
<td>asc route</td>
<td>Manage static routes.</td>
</tr>
<tr>
<td>asc service</td>
<td>Manage generic services.</td>
</tr>
<tr>
<td>asc ssh</td>
<td>Manage the SSH proxy.</td>
</tr>
<tr>
<td>asc upgrade</td>
<td>Apply software updates and license keys.</td>
</tr>
</tbody>
</table>
asc auth

Perform user authentication and authorization tests.

Syntax

asc auth [options]

Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h, --help</td>
<td>Display usage text.</td>
</tr>
<tr>
<td>-i, --iterations &lt;count&gt;</td>
<td>Repeat the authentication or authorization test the specified number of times. The value for &lt;count&gt; must be an integer. Default is 1.</td>
</tr>
<tr>
<td>-l, --listoperations</td>
<td>List all authorization test operations.</td>
</tr>
<tr>
<td>-o, --operation &lt;op&gt;</td>
<td>The operation to use for the authorization test. Note: The --target option is also required.</td>
</tr>
<tr>
<td>-p, --password &lt;password&gt;</td>
<td>The Active Directory user password. The password can also be specified using the HTFW environment variable.</td>
</tr>
<tr>
<td>-t, --target &lt;IP_address&gt;</td>
<td>The IP address of the protected host to use for policy and rules evaluation.</td>
</tr>
<tr>
<td>-u, --username &lt;username&gt;</td>
<td>The Active Directory username to test.</td>
</tr>
</tbody>
</table>

Examples

Authenticate the user joe:

    asc auth -u joe -p joespass

List all authentication and authorization test operations:

    asc auth -l

Authorize the xyz operation for the user abc on the host 10.1.10.105:

    asc auth -u abc -o xyz -t 10.1.10.105

asc backup

Perform backup and restore of the HTA configuration to facilitate disaster recovery and configuration migration.
Syntax

```
asc backup [options]
```

Options

**Table G-3 Options for asc backup command**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-b, --backup [file]</code></td>
<td>Create a configuration backup archive. The archive filename can be optionally specified.</td>
</tr>
<tr>
<td><code>-h, --help</code></td>
<td>Display usage text.</td>
</tr>
<tr>
<td><code>-n, --nocrypt</code></td>
<td>Create an unencrypted backup image. Unencrypted backup data must be stored and transported securely.</td>
</tr>
<tr>
<td><code>-p, --password &lt;password&gt;</code></td>
<td>Set or verify the configuration backup archive password.</td>
</tr>
<tr>
<td></td>
<td>The configuration backup archive password can also be specified using the <code>PASSWORD</code> environment variable.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This option is required to restore an archive if a password was specified when creating the archive.</td>
</tr>
<tr>
<td><code>-r, --restore [file]</code></td>
<td>Restore a configuration backup archive. This option uses the CD-ROM by default or takes an optional backup ISO filename.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The <code>--password</code> argument or environment variable is required if the archive is encrypted.</td>
</tr>
<tr>
<td><code>-t, --test</code></td>
<td>Validate the command line arguments without performing any actions.</td>
</tr>
<tr>
<td><code>-v, --verify [file]</code></td>
<td>Validate the configuration backup archive file. This option uses the CD-ROM by default or takes an optional backup ISO filename.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The <code>--password</code> argument or environment variable is required if the archive is encrypted.</td>
</tr>
</tbody>
</table>

Examples

Create an encrypted backup with a specified filename:

```
asc backup --backup /tmp/20120515_backup.iso --password 'secret123!'
```

Create an encrypted backup with the default filename:

```
export PASSWORD='secret123!'
asc backup --backup
```

Create an unencrypted backup with the default filename:
asc certs

    asc backup --backup --nocrpt

Validate a backup file:
    asc backup --verify /tmp/20120515_backup.iso --password 'secret123!'

Validate a backup on the CD-ROM:
    asc backup --verify --password 'secret123!'

Restore an encrypted backup file:
    asc backup --restore /tmp/20120515_backup.iso --password 'secret123!'

Restore an encrypted backup from the CD-ROM:
    asc backup --restore --password 'secret123!'
    or
    export PASSWORD='secret123!'  
    asc backup --restore

asc certs

Perform certificate and license key management.

Syntax

    asc certs [options]

Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a, --authority</td>
<td>Use this option when performing operations on a certificate authority (CA) certificate.</td>
</tr>
<tr>
<td>-c, --cert [file]</td>
<td>The fully qualified certificate target file path.</td>
</tr>
<tr>
<td></td>
<td>The contents of this file are overwritten.</td>
</tr>
<tr>
<td></td>
<td>Specifying -c or --cert will define the certificate file location automatically.</td>
</tr>
<tr>
<td>-d, --delete &lt;service&gt;</td>
<td>Delete the specified CA certificate by service name.</td>
</tr>
<tr>
<td></td>
<td>Implies --authority.</td>
</tr>
<tr>
<td>-g, --genselfsigned [file]</td>
<td>Generate a self-signed certificate using a local key.</td>
</tr>
<tr>
<td></td>
<td>This option accepts a temporary fully qualified filename as an argument with certificate data as contents. See --c or --csr help text for file content syntax.</td>
</tr>
<tr>
<td>-h, --help</td>
<td>Display usage text.</td>
</tr>
</tbody>
</table>
### Options for asc certs command (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| -i, --import <file> | Validate and install a certificate issued by a CA.  
**Note:** The `-s` option is also required. |
| -k, --key [file] | The fully qualified key target file path.  
The contents of this file are overwritten.  
Specifying the `-s` option defines the key file location automatically. |
| -l, --list | Lists the certificates installed locally and descriptions of each.  
List output is one certificate per line with each value separated by a double length underscore (`__`).  
The format is as follows:  
```
svc__t__cn__o__l__st__c__ou__exp__isd__s__icn__io__iou__v
```
Where:  
- `svn`—Service name. Valid values are:  
  - `log`  
  - `gui`  
- `t`—Type. Valid values are:  
  - `ss` (self-signed)  
  - `ext` (external)  
- `cn`—Common name  
- `o`—Organization  
- `l`—Locality  
- `st`—State/region  
- `c`—Country code  
- `ou`—Organizational unit  
- `exp`—Expiration date stamp OR the duration in days for CSR/self-signed generation  
- `isd`—Issued date stamp  
- `s`—Serial number (real certs only)  
- `icn`—Issuers common name  
- `io`—Issuers organization  
- `iou`—Issuers organizational unit  
- `key`—Key length in bits  
- `v`—TLS version
Examples

List all certificates installed:

```
asc certs -l
```

List all certificate authority (CA) certificates:

```
asc certs -l -a
```
Generate a certificate request for the HTA Logging service:

```
asc certs -s Log --csr /tmp/csrParams.txt
```

Validate and install a certificate for the HTA Management Console service:

```
asc certs -s GUI --import /tmp/newCert.pem
```

Export the current key and certificate to files:

```
asc certs -k /foo/mykey.pem -c /foo/ssCert.pem
```

Set the supported SSL version to SSLv2 and SSLv3:

```
asc certs -ssl 2
```

Set the supported SSL version to SSLv3 only:

```
asc certs -ssl 3
```

Delete the ca0025 service certificate authority certificate:

```
asc certs -a -d ca0025
```

Generate a 32 character random string:

```
asc certs -r 32
```

---

**asc firewall**

Perform firewall service management.

**Syntax**

```
asc firewall [options]
```

**Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a, --add &lt;IP_address&gt;</td>
<td>Add the specified protected host to the firewall.</td>
</tr>
<tr>
<td>-c, --class [x]</td>
<td>The type of host to be protected. This option defines the default proxy and forward settings for the specified class type. The x option implies a source rule exception.</td>
</tr>
<tr>
<td>-cp, --closeport &lt;port&gt;</td>
<td>Block access to the specified local TCP and UDP ports on the appliance.</td>
</tr>
<tr>
<td>-h, --help</td>
<td>Display usage text.</td>
</tr>
<tr>
<td>-l, --list</td>
<td>Lists all protected hosts, proxy redirects, and port forwards. This can be combined with the -class option to filter results.</td>
</tr>
</tbody>
</table>
Examples

Add an IP address proxy exception. (This IP address will not be proxied.):

```
asc firewall -a 1.2.3.4 -c x
```

List all firewall exception IP addresses:

```
asc firewall -l -c x
```

Remove a firewall exception by IP address:

```
asc firewall -r 1.2.3.4
```

Disable access to port 8091:

```
asc firewall -cp 8091
```

Enable access to port 8091:

```
asc firewall -op 8091
```

asc ha

Perform OS and application-level High Availability (HA) management on the HTA.

Syntax

```
asc ha [options]
```

Options

Table G-6 Options for asc ha command

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d, --disband</td>
<td>Disconnect the HTA from the HA cluster. This can be run from the primary or secondary HTA.</td>
</tr>
<tr>
<td>-e, --peertest</td>
<td>Test the health of the remote system and automatically failover if needed.</td>
</tr>
</tbody>
</table>
Table G-6  Options for asc ha command (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-f, --failover {auto</td>
<td>manual}</td>
</tr>
<tr>
<td></td>
<td>■ auto—Enable automatic failover. The secondary HTA can assume primary</td>
</tr>
<tr>
<td></td>
<td>functions if the primary HTA has been offline for the timeout interval.</td>
</tr>
<tr>
<td></td>
<td>■ manual—Disable automatic failover.</td>
</tr>
<tr>
<td>-h, --help</td>
<td>Display usage text.</td>
</tr>
<tr>
<td>--haclean</td>
<td>Clean old HA sync data keeping only the three most recent data sets.</td>
</tr>
<tr>
<td>-i, --interval &lt;minutes&gt;</td>
<td>Sets the data synchronization period, in minutes, between HTAs. Valid range is 2–1440.</td>
</tr>
<tr>
<td>-j, --join &lt;IP_address&gt;</td>
<td>Join two HTAs to create an HA cluster. This can be run from either the primary or secondary HTA.</td>
</tr>
<tr>
<td>-o, --mode {primary</td>
<td>secondary}</td>
</tr>
<tr>
<td></td>
<td>■ primary—The main HTA where all traffic is routed.</td>
</tr>
<tr>
<td></td>
<td>■ secondary—The backup or standby HTA.</td>
</tr>
<tr>
<td>Note:</td>
<td>Changing the HA mode triggers a failover event.</td>
</tr>
<tr>
<td>-p, --password &lt;password&gt;</td>
<td>The password of the remote HTA. Required when joining an HA cluster. Optionally, the password can be supplied via the HTHAPW environment variable.</td>
</tr>
<tr>
<td>-s, --sync</td>
<td>Force an immediate synchronization of data between HA HTAs.</td>
</tr>
<tr>
<td>--sshkeytest</td>
<td>Test the network connection between the two HA HTAs and verify the SSH keys</td>
</tr>
<tr>
<td>-t, --status</td>
<td>View the current configuration and operational state of the HA cluster.</td>
</tr>
<tr>
<td>-u, --timeout &lt;minutes&gt;</td>
<td>Set the primary HTA monitoring minimum time threshold, in minutes, before an automatic failover event occurs.</td>
</tr>
<tr>
<td>-v, --pollinterval</td>
<td>Set the health monitoring period, in seconds, before automatic failover mode is enabled.</td>
</tr>
</tbody>
</table>

Examples

Trigger a failover event from the secondary node:

```
asc ha --mode primary
```

Synchronize and trigger a failover event from the primary node:

```
asc ha --sync --mode secondary
```

View the HA configuration and status:
asc ha --status

Create an HA cluster from the secondary HTA:
asc ha --join 10.1.0.100 --password s3crEt --mode secondary

Create an HA cluster from the primary HTA:
asc ha --join 10.1.0.100 --password s3crEt --mode primary

Leave the HA cluster from the secondary HTA:
asc ha --disband

Enable automatic failover:
asc ha --failover auto

Disable automatic failover:
asc ha --failover manual

asc log

Perform HTA system logging management.

Syntax

asc log [options]

Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-f, --full</td>
<td>An optional argument to include all log data, not just recent log data.</td>
</tr>
<tr>
<td></td>
<td>Only works with --troubleshoot.</td>
</tr>
<tr>
<td>-h, --help</td>
<td>Display usage text.</td>
</tr>
<tr>
<td>-l, --level &lt;level&gt;</td>
<td>Specifies which messages to export to the remote logging servers. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>■ 0 or emerg</td>
</tr>
<tr>
<td></td>
<td>■ 1 or alert</td>
</tr>
<tr>
<td></td>
<td>■ 2 or crit</td>
</tr>
<tr>
<td></td>
<td>■ 3 or err</td>
</tr>
<tr>
<td></td>
<td>■ 4 or warning</td>
</tr>
<tr>
<td></td>
<td>■ 5 or notice</td>
</tr>
<tr>
<td></td>
<td>■ 6 or info</td>
</tr>
<tr>
<td></td>
<td>■ 7 or debug</td>
</tr>
<tr>
<td>Note:</td>
<td>Either the number or the text can be used.</td>
</tr>
</tbody>
</table>
**Examples**

Permanently delete all system and audit logs:

```plaintext
asc log -p
```

Set a remote Syslog server and use TLS encryption:

```plaintext
asc log -s logger.company.com -x
```

Set two remote Syslog servers, the log level, and no encryption:

```plaintext
asc log -s log1.company.com -s log2.company.com -l warning
```

Stop remote logging:

```plaintext
asc log -r
```

Set the logging level to *notice*:

```plaintext
asc log -l 5
```

or

```plaintext
asc log -l notice
```

Create a troubleshooting file for HyTrust Support diagnostics and include all log data:

```plaintext
asc log -t -f
```

Create a small troubleshooting file with recent log data only:

```plaintext
asc log -t
```
asc monitor

asc monitor

Perform HTA monitoring management.

Syntax

asc monitor [options]

Options

<table>
<thead>
<tr>
<th>Table G-8</th>
<th>Options for asc monitor command</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option</strong></td>
<td>Description</td>
</tr>
<tr>
<td>-a, --fileaudit</td>
<td>Audit the local filesystem to identify possible intrusions. This feature invokes the Advanced Intrusion Detection Environment (AIDE) using HTA validated reference data.</td>
</tr>
<tr>
<td>-c, --community &lt;string&gt;</td>
<td>Specify the SNMP community string.</td>
</tr>
<tr>
<td>-e, --email &lt;email_address&gt;</td>
<td>Set an email address where system notifications will be sent.</td>
</tr>
<tr>
<td>-f, --force</td>
<td>Ignore failed connection attempts to mail servers and SNMP trap recipient hosts.</td>
</tr>
<tr>
<td>-H, --health</td>
<td>Perform a health check on the HTA.</td>
</tr>
<tr>
<td>-h, --help</td>
<td>Display usage text.</td>
</tr>
<tr>
<td>-k, --network {on</td>
<td>off}</td>
</tr>
<tr>
<td>-l, --trial</td>
<td>Send an SNMP and SMTP test alert notice. Include the --message option to send a specific message.</td>
</tr>
<tr>
<td>-m, --message &lt;message&gt;</td>
<td>Specify the message to use in log files and configuration file change journals for monitoring related activities.</td>
</tr>
<tr>
<td>-n, --snmp {on</td>
<td>off}</td>
</tr>
<tr>
<td>-p, --protected {on</td>
<td>off}</td>
</tr>
<tr>
<td>-s, --server &lt;smtp_server&gt;</td>
<td>Set the SMTP server to use for sending email notifications.</td>
</tr>
<tr>
<td>-t, --trap &lt;trap_host&gt;</td>
<td>Set an SNMP Trap recipient host.</td>
</tr>
<tr>
<td>-u, --status</td>
<td>Display a report showing service, resource state, and monitoring configuration.</td>
</tr>
</tbody>
</table>
Examples

Set the SMTP notification server and target address:

asc monitor -s mail.foo.com -e user@foo.com

Enable the SNMP server and set its community and trap recipient host:

asc monitor -n on -c public -t 1.2.3.4

Send an SMTP and SNMP test with a message:

asc monitor -l -m "Hello monitoring systems"

View a system status report:

asc monitor --status

Set an SMTP server:

asc monitor -s smtp.foo.com

Set a single SNMP Trap recipient host:

asc monitor -t trapd.foo.com

Set two SNMP Trap recipient hosts:

asc monitor -t trapd.foo.com -t trapd2.foo.com

Enable the SNMP server:

asc monitor -n on

Disable the SNMP server:

asc monitor -n off

Set the SNMP community string:

asc monitor -c public

or

asc monitor -c othercommunity

Specify a single email address where notifications will be sent:

asc monitor -e admin@foo.com

Specify three email addresses where notification will be sent:

asc monitor -e admin@foo.com -e other@foo.com -e third@elsewhere.org

Perform an audit of the local HTA filesystem:

asc monitor --fileaudit

Disable network resource monitoring (NRM):

asc monitor --network off

Disable protected host monitoring (PHM):

asc monitor --protected off

asc network

Perform HTA network resource management.
## Syntax

`asc network [options]`

### Options

**Table G-9 Options for asc network command**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--ads</td>
<td>Update the Active Directory Service configuration to synchronize with the HTA Management Console settings. This may change computer records on the Active Directory server.</td>
</tr>
<tr>
<td>-d, --disable</td>
<td>Disable a network device.</td>
</tr>
<tr>
<td>-dn, --domainname &lt;domain&gt;</td>
<td>Set the domain name. Multiple domain names can be specified to define the host lookup domain search suffixes.</td>
</tr>
<tr>
<td>-e, --enable</td>
<td>Enable a network device.</td>
</tr>
<tr>
<td>-gw, --gateway &lt;gateway&gt;</td>
<td>Define the default gateway for a network device.</td>
</tr>
<tr>
<td>-h, --help</td>
<td>Display usage text.</td>
</tr>
<tr>
<td>-hn, --hostname &lt;name&gt;</td>
<td>Set the unqualified hostname.</td>
</tr>
<tr>
<td>-i, --interface &lt;device&gt;</td>
<td>The name of the network device to configure. The interface name <code>prod</code> can be used to imply either br0 or bond0 depending on what network topology has been selected.</td>
</tr>
<tr>
<td>-ip, --ipaddress</td>
<td>Specify the IPv4 address or the text <code>dhcp</code> as an argument.</td>
</tr>
<tr>
<td>-m, --message &lt;message&gt;</td>
<td>Specify the message to use in log files and configuration file change journals for network related activities.</td>
</tr>
<tr>
<td>-nm, --netmask &lt;mask&gt;</td>
<td>Set the subnet mask.</td>
</tr>
<tr>
<td>-ns, --nameserver &lt;nameserver&gt;</td>
<td>Set the name servers. Up to three name servers are supported.</td>
</tr>
<tr>
<td>-s, --status</td>
<td>Display network device status. Use the <code>--interface</code> option to only show status for a specific device.</td>
</tr>
</tbody>
</table>
Examples

Set the IP address, subnet mask and gateway for the eth0 network device:
   asc network -i eth0 -ip 1.2.3.4 -nm 255.255.255.0 -gw 1.2.3.254

Set the hostname, domain name, and two name servers for the HTA:
   asc network -hn asc01 -dn example.com -ns 1.1.1.1 -ns 1.2.3.4

Enable the br0 network device and set it to acquire an IP address via DHCP:
   asc network -i br0 -ip dhcp --enable

Retrieve the status of the br0 network device:
   asc network -i br0 --status

Disable the br0 network device:
   asc network -i br0 --disable

Set the network topology to bridge mode:
   asc network -t bridge

Set the network topology to proxy mode:
   asc network -t proxy

Set the network topology to router mode:
   asc network -t router

Set three domain names for the HTA
   asc network -dn example.com -dn dept.example.com -dn search.org

Set the hostname for the HTA:
   asc network -hn asc01

Enable the spanning tree protocol:
   asc network -stp on
asc policy

Disable the spanning tree protocol:

asc network -stp off

asc policy

Perform HTA policy management.

Syntax

asc policy [options]

Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h, --help</td>
<td>Display usage text.</td>
</tr>
<tr>
<td>-p, --purge &lt;days&gt;</td>
<td>Delete policy data older than the specified number of days. The value for</td>
</tr>
<tr>
<td></td>
<td>&lt;days&gt; must be an integer greater than 7.</td>
</tr>
<tr>
<td>-r, --refreshsco {true</td>
<td>false}</td>
</tr>
<tr>
<td></td>
<td>data after Structure Changing Operations (SCO) are authorized.</td>
</tr>
<tr>
<td>-s, --status</td>
<td>Display the existing policy settings.</td>
</tr>
</tbody>
</table>

Examples

List the current policy settings:

asc policy -s

Disable Structure Changing Operation (SCO) automatic refresh:

asc policy -r false

Enable Structure Changing Operation (SCO) automatic refresh:

asc policy -r true

asc route

Perform HTA static route management.

Syntax

asc route [options]
Options

Table G-11 Options for asc route command

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a, --add &lt;IP address&gt;/&lt;mask&gt;:&lt;gateway&gt;</td>
<td>Add a static route.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The --interface option is required.</td>
</tr>
<tr>
<td>-b, --bgp {on</td>
<td>off}</td>
</tr>
<tr>
<td>-e, --edit &lt;IP address&gt;/&lt;mask&gt;:&lt;gateway&gt;</td>
<td>Modify an existing static route.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The --interface option is required.</td>
</tr>
<tr>
<td>-f, --ospf {on</td>
<td>off}</td>
</tr>
<tr>
<td>-h, --help</td>
<td>Display usage text.</td>
</tr>
<tr>
<td>-i, --interface &lt;device&gt;</td>
<td>The name of the network device to configure.</td>
</tr>
<tr>
<td>-l, --list</td>
<td>Display the current static route configuration.</td>
</tr>
<tr>
<td></td>
<td>Use the --interface option to only show static routes for a specific device.</td>
</tr>
<tr>
<td>-m, --message &lt;message&gt;</td>
<td>Specify the message to use in log files and configuration file change journals for static route related activities.</td>
</tr>
<tr>
<td>-n, --rip {on</td>
<td>off}</td>
</tr>
<tr>
<td>-o, --old &lt;IP address&gt;/&lt;mask&gt;:&lt;gateway&gt;</td>
<td>The original route to be replaced by an edited route.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The --interface option is required.</td>
</tr>
<tr>
<td>-p, --password</td>
<td>The password to use to authenticate route management services.</td>
</tr>
<tr>
<td>-r, --del &lt;IP address&gt;/&lt;mask&gt;:&lt;gateway&gt;</td>
<td>Delete a static route.</td>
</tr>
</tbody>
</table>

Examples

Add a static route to network 1.2.3.0/255.255.255.0 via eth0, with gateway 10.20.30.1:

```
asc route -a 1.2.3.0/255.255.255.0:10.20.30.1 -i eth0
```

or

```
asc route -a 1.2.3.4/24:10.20.30.1:eth0
```

Remove a static route to network 1.2.3.0/255.255.255.0:

```
asc route -r 1.2.3.0/255.255.255.0
```

or
asc service

    asc route -r 1.2.3.0/24

List all static routes:
    asc route -l

List static routes for the interface eth0:
    asc route -l -i eth0

Edit an existing static route:
    asc route -e 1.2.3.0/255.255.255.0:10.20.30.1 -i eth0
    or
    asc route -e 1.2.3.4/24:10.20.30.1:eth0

Enable BGP:
    asc route --bgp on

Disable BGP:
    asc route --bgp off

Enable RIP:
    asc route --rip on

Disable RIP:
    asc route --rip off

Specify a password to use for route management services:
    asc route --password /tmp/passwordfile.txt

asc service

Perform generic HTA service management and simple configuration file changes.

Syntax

    asc service [options]

Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d, --disable</td>
<td>Disable a service.</td>
</tr>
<tr>
<td>-e, --enable</td>
<td>Enable a service.</td>
</tr>
<tr>
<td>-f, --configfile &lt;file&gt;</td>
<td>Specify the configuration file(s) to read or modify. Multiple files can be specified. Searches and changes are processed to each file in the order specified.</td>
</tr>
</tbody>
</table>

Note: The --servicename option is required.
### Examples

**Change the check-files setting for the NSC service and enable/restart it:**

```
asc service -n nscd -f /etc/nscd.conf -e -p "check-files=group no"
```

**Search the NTP configuration file and display all "server" parameter values:**

```
asc service -f /etc/ntp.conf -p "server"
```

**Search the NTP, NSC, and DNS resolver configuration files and display all "server" parameter values:**

```
asc service -f /etc/ntp.conf -f /etc/nscd.conf -f /etc/resolv.conf -p "server"
```

**Change the first NTP server and restart the NTP service:**

```
asc service -n ntpd -f /etc/ntp.conf -e -p "server=ntp.server.your.com"
```

**Disable the NTP, Tomcat, and PostgresSQL services:**

```
asc service -d -n ntpd -n postgresql -n tomcat6
```

**Set the first NTP server, delete the second and third, and change the restrict parameter value:**

```
asc service -f /etc/ntp.cnf -p server=ntp1.example.com -p server=%% -p server=%% -p "restrict=default kod nomodify"
```

**Specify multiple services to manage:**

```
asc service -h, --help
```

```command
Display usage text.
```

```command
-m, --message <message>
```

```command
Specify the message to use in log files and configuration file change journals for service related activities.
```

```command
-n, --servicename <service>
```

```command
The name of the service to manage.
The name must match the name of the service init script in the directory /etc/init.d/.
Multiple service names can be specified and are managed in the order specified.
```

```command
-p, --parameter <string>
```

```command
The parameter to read or change in the specified configuration file.
**Note:** The --configfile option is required.
**Note:** To delete a parameter, set the new value to %% (e.g., "param=%%").
```

```command
-R, --reboot
```

```command
Reboot the HTA.
```

```command
-r, --revert
```

```command
Revert the specified configuration file parameters to their previous value.
**Note:** The --configfile option is required.
**Note:** This option cannot be used with the --parameter option.
```

```command
-v, --verbose
```

```command
Enable verbose output.
```

```command
-vv
```

```command
Enable debug output.
```
**asc ssh**

Perform HTA SSH Proxy service management.

**Syntax**

```
asc ssh [options]
```

**Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-a, --add &lt;command&gt;</code></td>
<td>Add a custom command and its associated operation. Note: The <code>--operation</code> option is required.</td>
</tr>
<tr>
<td><code>-d, --disable</code></td>
<td>Disable the SSH Proxy.</td>
</tr>
<tr>
<td><code>-e, --enable</code></td>
<td>Enable the SSH Proxy or reload its configuration if it is already running.</td>
</tr>
<tr>
<td><code>-h, --help</code></td>
<td>Display usage text.</td>
</tr>
<tr>
<td><code>-l, --list</code></td>
<td>Display all custom commands and their associated operations. Use with the <code>--operation</code> option to list all known operations.</td>
</tr>
<tr>
<td><code>-o, --operation [&lt;op&gt;]</code></td>
<td>List, add, or remove custom SSH command operations. Used with the <code>--list, --add, or --remove</code> options.</td>
</tr>
<tr>
<td><code>-r, --remove &lt;command&gt;</code></td>
<td>Remove a custom command.</td>
</tr>
<tr>
<td>`-s, --stream {on</td>
<td>off}`</td>
</tr>
</tbody>
</table>

**Examples**

List all custom user commands and their associated operations:
```
asc ssh -l
```

Lists all known operations:
```
asc ssh -l -o
```

Search for unknown commands in the SSH Proxy log:
```
asc ssh -f
```

Add a custom command associated with the *whitelist* operation:
asc ssh -a "/bin/date" -o " whitelist"

Remove the custom command "/bin/date":

asc ssh -r "/bin/date"

Disable the stream log:

asc ssh -s on

Disable the SSH Proxy service:

asc ssh -d

asc upgrade

Perform software updates and license key management.

Syntax

asc upgrade [options]

Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d, --db</td>
<td>Update version data in the local database for GUI reference.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This option is implied by both --iso and --version options.</td>
</tr>
<tr>
<td>-h, --help</td>
<td>Display usage text.</td>
</tr>
<tr>
<td>-i, --iso [iso_file]</td>
<td>Use a virtual DVD-ROM device or local ISO image file.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The --db option is implied.</td>
</tr>
<tr>
<td>-m, --message &lt;message&gt;</td>
<td>Specify the message to use in log files and configuration file change journals for upgrade related activities.</td>
</tr>
<tr>
<td>-v, --version &lt;version&gt;</td>
<td>Upgrade to the specified version.</td>
</tr>
</tbody>
</table>

Where version = major.minor.svn_id.

**Note:** All intermediate upgrades, if located in the same location, are installed automatically.

**Note:** The --db option is implied.

Examples

Upgrade using an attached ISO image:

asc upgrade -i

Upgrade to version 1.0.1974.
asc upgrade

    asc upgrade -v 1.0.1974

Upgrade using a local ISO image file:

    asc upgrade -i /tmp/UpgradeFile.iso

Upgrade to version 1.1.5000 and add a message to the log file:

    asc upgrade -v 1.1.5000 -m "Upgrade by Jane Doe through GUI"

Synchronize the local database version data with the installed version:

    asc upgrade -d