

IBM



# Technical Support Appliance Setup Guide

*Version 1 Release 5*



IBM



# Technical Support Appliance Setup Guide

*Version 1 Release 5*

**Note**

Before using this information and the product it supports, read the information in "Notices" on page 61.

Sixth edition (August 2013)

This edition applies to version 1, release 4, modification 0 of IBM Technical Support Appliance and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2011, 2013.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

# Contents

## Chapter 1. Introduction . . . . . 1

User accounts and user groups . . . . .	1
Discovery Scopes and Scope Sets . . . . .	2
Discovery credentials . . . . .	2
Discovery anchors . . . . .	3
Discovery gateways . . . . .	3
Discovery schedule . . . . .	3
Transmission schedule . . . . .	3

## Chapter 2. Prerequisites . . . . . 5

Required internet browsers . . . . .	5
Configuration requirements for connections to IBM Support . . . . .	5
Credential and software requirements for the discovery environment . . . . .	6

## Chapter 3. Setting up the Technical Support Appliance . . . . . 7

Connecting and powering on the Technical Support Appliance . . . . .	7
Assigning a static IP address to the Technical Support Appliance . . . . .	8
Logging in to the Technical Support Appliance . . . . .	9
Registering the Technical Support Appliance . . . . .	10
Setting the clock . . . . .	11
Configuring network settings . . . . .	12
Configuring basic network settings . . . . .	12
Configuring advanced network settings . . . . .	13
Setting up IBM connectivity . . . . .	16
Updating the Technical Support Appliance . . . . .	17
Installing an SSL server certificate . . . . .	17
Setting up user accounts and user groups . . . . .	18
Setting up a user group . . . . .	18
Setting up a user account . . . . .	19
Setting up discovery Scopes . . . . .	20
Setting up discovery credentials . . . . .	21
Configuring key pair authentication . . . . .	23
Setting up discovery anchors . . . . .	25
Modifying the discovery schedule . . . . .	26
Running the discovery . . . . .	26
Running the discovery on specific scope sets . . . . .	26
Running discovery on specific scopes . . . . .	27
Modifying the transmission schedule . . . . .	27
Running the transmission . . . . .	28

## Chapter 4. Using the Technical Support Appliance . . . . . 29

User accounts and user groups . . . . .	29
Displaying user accounts and user groups . . . . .	29
Adding user accounts and user groups . . . . .	29
Modifying user accounts and user groups . . . . .	31
Deleting user accounts and user groups . . . . .	32
Discovery Scopes . . . . .	33
Displaying discovery Scopes and Scope Sets . . . . .	33

Adding discovery Scopes . . . . .	33
Modifying a discovery Scope Set . . . . .	35
Deleting discovery Scopes . . . . .	36
Discovery credentials . . . . .	37
Displaying credentials . . . . .	37
Viewing credential details . . . . .	37
Adding credentials . . . . .	37
Modifying credentials . . . . .	39
Deleting credentials . . . . .	40
Discovery anchors . . . . .	40
Displaying anchors . . . . .	40
Editing the anchor port . . . . .	40
Adding anchors . . . . .	41
Modifying anchors . . . . .	41
Deleting anchors . . . . .	42
Discovery gateways . . . . .	42
Displaying discovery gateways . . . . .	42
Modifying discovery gateways . . . . .	42
Deleting gateways . . . . .	43
Discovery schedule . . . . .	43
Viewing the discovery schedule . . . . .	43
Modifying the discovery schedule . . . . .	44
Disabling the discovery schedule . . . . .	44
Running the discovery . . . . .	45
Saving the discovered data collection . . . . .	45
Discovery history . . . . .	46
Transmission schedule . . . . .	46
Viewing the transmission schedule . . . . .	46
Modifying the transmission schedule . . . . .	47
Disabling the transmission schedule . . . . .	47
Running the transmission . . . . .	47
Status information . . . . .	48
Viewing the activity log . . . . .	48
Viewing the inventory report . . . . .	49
Passwords . . . . .	49
Changing your password . . . . .	49
Security . . . . .	49
Configuring key pair authentication . . . . .	50
Installing an SSL server certificate . . . . .	52
Modifying session timeout settings . . . . .	52
Backup and restore . . . . .	53
Update . . . . .	54
Logging and trace . . . . .	54
Shutdown . . . . .	55
Tools . . . . .	56
Network Tools . . . . .	56
Unknown Devices . . . . .	57
Advanced Storage . . . . .	57

## Accessibility . . . . . 59

## Notices . . . . . 61

Trademarks . . . . .	62
----------------------	----



---

## Chapter 1. Introduction

The Technical Support Appliance is an easy-to-use tool that enables you to get more value from your IBM® Support contracts. The Technical Support Appliance discovers key information technology elements and their relationships within your IT infrastructure. Then, the Technical Support Appliance securely transmits the data to IBM Support for analysis. This data provides IBM Support with insight into the complex relationships between the applications, middleware, servers, and network components in your data center.

The Technical Support Appliance includes a web-based user interface (UI) that you can use to set up and customize access to your system and data. The UI also enables you to modify schedules for data discovery and transmission.

**Note:** As part of the discovery process the Technical Support Appliance initially attempts to detect endpoints within the defined scope without using discovery credentials. This involves the use of NMap and attempts to discover and classify devices with minimally intrusive IP scanning, stack fingerprinting, and port mapping. Generally, this activity is not significant enough to set off an intrusion detection system (IDS), but might do so if there are stringent local settings.

---

### User accounts and user groups

Executing any Technical Support Appliance function requires a certain authority level. If an authenticated user attempts to perform a function without the appropriate authority level, an error is displayed and the function is not executed.

Within an organization, roles can be created for various job functions. The permissions to perform certain operations are assigned to specific roles. System users are assigned particular roles, and through those role assignments have the necessary permissions to perform particular system functions. That way, any user assigned to a role will have the authority levels associated with that role and it is easy to add a user to a role, to change users from one role to another, or to remove users from a role.

In the Technical Support Appliance, roles are managed with user groups that have associated authority levels. Users are managed with user accounts. User accounts can be assigned membership in one or more user groups, and through those memberships, users have the authority level to perform particular functions.

In addition, user groups can be further restricted to selected scope sets. A scope set is a collection of IP addresses, address ranges, or subnets that identify the IT elements that the Technical Support Appliance can discover. Specifying scope set restrictions for a user group is a way to further limit access of the members of that user group. For example, it is possible to create platform-specific user groups, such as users responsible for maintaining Linux systems, through a combination of authority level and scope set restrictions associated with a particular user group.

**Related concepts:**

“Discovery Scopes and Scope Sets”

Discovery Scopes identify the resources that you want the Technical Support Appliance to discover. Discovery Scopes are grouped into discovery Scope Sets.

---

## Discovery Scopes and Scope Sets

Discovery Scopes identify the resources that you want the Technical Support Appliance to discover. Discovery Scopes are grouped into discovery Scope Sets.

You can specify discovery Scopes by using an IP address, a range of IP addresses, or a network or subnet to define the resources that are accessed during discovery. A discovery Scope can be as small as a single IP address, or as large as a range of IP addresses or a network.

The more IP addresses that are in the discovery Scope, the longer the discovery takes. You can modify the discovery size by disabling or enabling discovery Scope Sets or by excluding IP addresses, ranges of IP addresses, or networks or subnets from a Scope within a Scope Set.

**Related tasks:**

“Adding user accounts and user groups” on page 29

You can add user accounts and groups to control access to Technical Support Appliance functions.

---

## Discovery credentials

Discovery credentials are a collection of user names, passwords, and Simple Network Management Protocol (SNMP) community strings that the Technical Support Appliance uses to access resources during the discovery.

You must set up and maintain discovery credentials for the resources that you want to discover. The access information that you provide varies by the type of credential, but usually includes at least user name and password.

When accessing a resource, the Technical Support Appliance sequentially uses each credential across a particular scope in the order that is listed on the Discovery Credentials page until the resource allows the Technical Support Appliance permission to access it. For example, when accessing a computer system, the Technical Support Appliance uses the first user name and password that is specified in the credential list for computer systems. If the user name and password are incorrect for a particular computer system, the Technical Support Appliance automatically uses the next user name and password that is specified in the computer list for computer systems.

You can restrict discovery credentials to be used only when the Technical Support Appliance is discovering a particular scope set. This restriction improves performance and prevents invalid login attempts that can result in the account becoming locked.

**Tip:** Create a service account to be used across each installed instance of a certain type, such as Windows or WebSphere® Application Server. If you have only one password for all instances of a certain type, then you must specify only the discovery credential one time.

---

## Discovery anchors

In order to perform a discovery, the Technical Support Appliance must be able to communicate with other computer hosts and network devices. When a firewall prevents direct access from the discovery server to certain hosts or devices, you can use a discovery proxy server that has access to these hosts or devices to enable the discovery. This discovery proxy server is called an anchor server or anchor.

The anchor must be in the same network section as the resources that you want to discover. Restrict the anchor server scope to the systems in that network section.

---

## Discovery gateways

A discovery gateway is a proxy server that has access to Microsoft Windows systems in your environment. Before Technical Support Appliance version 1, release 3, it was necessary to specify a Windows server as a discovery gateway before the Technical Support Appliance could discover information about systems that are running Microsoft Windows. With version 1, release 3, the Technical Support Appliance can discover this information without a discovery gateway. Any discovery gateways that are defined for prior releases of the Technical Support Appliance will continue to function.

---

## Discovery schedule

Discoveries run on scheduled days and times to ensure that discovered data is always current and accurate. The Technical Support Appliance has a default discovery schedule that you can modify for your needs. You can also view details, history, and the state of the last discovery that was run.

When you modify the discovery schedule, you specify the start time and the frequency of discoveries. You can also run discoveries on demand.

The duration of the discovery is dependent on a number of factors including the number of resources being accessed.

---

## Transmission schedule

Discovered data is securely packaged and transmitted to IBM Support on regularly scheduled days and times to ensure that IBM has the most current and accurate information. A default transmission schedule, that you can modify for your needs, is provided. You can also run transmissions on demand.

The transmission time varies depending on the amount of discovered data.



---

## Chapter 2. Prerequisites

Before beginning to set up and use the Technical Support Appliance, you need to ensure that you meet prerequisites, such as the required credentials for the discovery environment and configuration requirements for connecting to IBM Support.

---

### Required internet browsers

You use a web-based user interface to set up and monitor discovery and transmission.

The Technical Support Appliance supports the following internet browsers that are running on Microsoft Windows:

- Mozilla Firefox V17 Extended Support Release (ESR)
- Microsoft Internet Explorer V9.0 for Windows 7
- Microsoft Internet Explorer V8.0 for Windows XP

You can download these browsers from the following sites:

- Microsoft Internet Explorer (<http://www.microsoft.com/downloads/>)
- Mozilla Firefox (<http://www.mozilla.org/products/firefox/>)

---

### Configuration requirements for connections to IBM Support

The Technical Support Appliance can connect to IBM Support through a direct connection or through a user-supplied proxy that you must configure to allow communication with IBM.

For the Technical Support Appliance to communicate successfully, your external firewall must allow outbound connections on port 80 and port 443. On your firewall, you can choose to limit the specific IP addresses to which the Technical Support Appliance system can connect.

*Table 1. Network connections*

DNS name	IP address	Port	Purpose
www6.software.ibm.com	170.225.15.41	443	Transmission of discovery data
download4.boulder.ibm.com	170.225.15.107	80	Download of software update
download4.mul.ie.ibm.com	129.35.224.107	80	Download of software update
delivery04.dhe.ibm.com	129.35.224.105	80	Download of software update
delivery04.dhe.ibm.com	170.225.15.105	80	Download of software update
download3.boulder.ibm.com	170.225.15.76	80	Download of software update
download3.mul.ie.ibm.com	129.35.224.114	80	Download of software update

Table 1. Network connections (continued)

DNS name	IP address	Port	Purpose
eccgw01.boulder.ibm.com	207.25.252.197	443	Transmission of discovery data
eccgw02.rochester.ibm.com	129.42.160.51	443	Transmission of discovery data
www.ibm.com	129.42.56.216	443	Download of configuration update
www.ibm.com	129.42.58.216	443	Download of configuration update
www.ibm.com	129.42.60.216	443	Download of configuration update
www-03.ibm.com	204.146.30.17	443	Download of configuration update

---

## Credential and software requirements for the discovery environment

In order to discover endpoints or resources in your environment, the Technical Support Appliance must have access to those resources. It is recommended that you create a service account on each resource that is specifically for the Technical Support Appliance to use when accessing that resource.

After you create a service account on a resource, you must define and maintain credentials on the Technical Support Appliance that match the credentials defined on the resource for that service account. The Technical Support Appliance uses these credentials to access the resource. Requirements for credentials vary according to the environment and the type of resource that you want to discover, but typically include a user name and password. Some resources have specific software requirements as well.

For more information about credentials and software requirements, refer to "Endpoint Planning" in the IBM developerWorks® Tivoli® Application Dependency Discovery Manager wiki. You can access the wiki at the following web address:

[www.ibm.com/developerworks/mydeveloperworks/wikis/home/wiki/Tivoli%20Application%20Dependency%20Discovery%20Manager/page/Endpoint%20Planning](http://www.ibm.com/developerworks/mydeveloperworks/wikis/home/wiki/Tivoli%20Application%20Dependency%20Discovery%20Manager/page/Endpoint%20Planning)

### Related concepts:

"Discovery credentials" on page 2

Discovery credentials are a collection of user names, passwords, and Simple Network Management Protocol (SNMP) community strings that the Technical Support Appliance uses to access resources during the discovery.

---

## Chapter 3. Setting up the Technical Support Appliance

The Technical Support Appliance includes preinstalled software.

### About this task

Follow these steps to quickly get started with the Technical Support Appliance. If you have not already done so, review Chapter 2, “Prerequisites,” on page 5.

### Procedure

1. Connecting and powering on the Technical Support Appliance
2. (Optional) Assigning a static IP address to the Technical Support Appliance
3. “Logging in to the Technical Support Appliance” on page 9
4. “Registering the Technical Support Appliance” on page 10
5. Setting the clock
6. Configuring network settings
7. Setting up IBM connectivity
8. “Updating the Technical Support Appliance” on page 17
9. (Optional) Installing an SSL server certificate
10. “Setting up user accounts and user groups” on page 18
11. Setting up discovery scopes.
12. Setting up discovery credentials.
13. (Optional) Setting up discovery anchors
14. Modifying the discovery schedule.
15. Running the discovery.
16. Viewing the inventory report.
17. Modifying the transmission schedule.
18. Running the transmission.

### What to do next

When you finish setting up the Technical Support Appliance, see Chapter 4, “Using the Technical Support Appliance,” on page 29 for information about how to perform other tasks.

#### Related concepts:

Chapter 2, “Prerequisites,” on page 5

Before beginning to set up and use the Technical Support Appliance, you need to ensure that you meet prerequisites, such as the required credentials for the discovery environment and configuration requirements for connecting to IBM Support.

---

## Connecting and powering on the Technical Support Appliance

Before signing on to the Technical Support Appliance, you must ensure that it is connected and powered on.

## About this task

Follow these steps to connect and power on the Technical Support Appliance.

### Procedure

1. Before powering the system on, connect an Ethernet cable from Ethernet Port 1 to your local Ethernet.
2. Connect a monitor, USB mouse, and USB keyboard to the system.
3. Power on the system. The monitor displays several messages at startup. After several minutes, the startup tasks complete and the VMware ESXi display is shown.
4. Press F2 and enter pw4ibmtsa as the root password for ESXi.

**Note:** After you connect, it is recommended that you change this default root password. To change the password, use **Configure Password** on the VMware ESXi console.

---

## Assigning a static IP address to the Technical Support Appliance

The Technical Support Appliance runs on a virtual server on the host system and therefore requires its own IP address. If you have a DHCP server in your network, the DHCP server provides the IP address for the Technical Support Appliance. If you do not have a DHCP server in your network, you must assign a static IP address to the Technical Support Appliance.

### Procedure

To assign a static IP address for the Technical Support Appliance, follow these steps:

1. With the host system powered off, place an empty USB key into the first USB slot of the system.
2. Power on the host system.
3. Wait approximately 10 minutes for the system to start and write to the USB key. When this completes, the USB key contains a file that is called `ipconfig.properties`. The contents of this file are as follows:

```
# DISABLED={true | false} - if set to true, this file will be ignored.
DISABLED=true
# IPTYPE={static | dhcp}
IPTYPE=dhcp
# HOSTNAME=<hostname of system>
HOSTNAME=ibmtsa
# IPADDR=<ip address of system(only for static)>

# NETMASK=<ip mask of network(only for static)>

# GATEWAY=<ip address of gateway(only for static)>

# DOMAIN=<network domain of system for DNS usage(optional)>

# DNS1=<name of first DNS server(optional)>

# DNS2=<name of second DNS server(optional)>

# DNS3=<name of third DNS server(optional)>
```

4. Modify the `ipconfig.properties` file to specify the configuration you want to use.

Table 2. Configuration file examples

IP type	Example configuration file properties
DHCP	DISABLED=false IPTYPE=dhcp HOSTNAME=ibmtsa  <b>Note:</b> In most DHCP applications, the DOMAIN and DNS servers are not set as they are provided by the DHCP server.
Static	DISABLED=false IPTYPE=static HOSTNAME=ibmtsa IPADDR=192.168.2.3 NETMASK=255.255.255.0 GATEWAY=192.168.2.1 DOMAIN=ourcompany.com DNS1=192.168.3.200 DNS2=192.168.3.100

5. To put the TCP/IP changes on the Technical Support Appliance, follow these steps:
  - a. Power off the Technical Support Appliance.
  - b. With the host system powered off, place an empty USB key into the first USB slot on the front of the system.
  - c. Power on the host system.

After several minutes, the Technical Support Appliance restarts with the new configuration.

---

## Logging in to the Technical Support Appliance

Log in to the Technical Support Appliance web user interface with the administrator user ID and password.

### About this task

To log in to the Technical Support Appliance web user interface, follow these steps:

### Procedure

1. Open an internet browser from a device on the same network as the Technical Support Appliance. For information about the internet browsers you can use for the Technical Support Appliance, see “Required internet browsers” on page 5.
2. Enter the following URL in the browser Address bar:  
https://ibmtsa/appliance
3. When prompted, enter the following information:

**User ID:**

Enter admin

**Password:**

Enter the Technical Support Appliance administrator password.

The initial Technical Support Appliance administrator password that is provided is `passw0rd`. You must change this initial password after you use it to log in to the Technical Support Appliance.

To change the initial password, follow these steps:

- a. Enter a new password.  
The password must adhere to the following rules:
  - Must be at least 8 characters long
  - Must contain at least one alphabetic and one non-alphabetic character
  - Must not contain the user name
  - Must not be the same as any of the previous eight passwords
  - Must be changed at least once every 90 days, but must not be changed more than once each day
- b. Enter the new password again in the **Confirm password** field. The two passwords that you enter are compared to confirm that they match before the password is saved.
- c. Record the new password for future reference.

**Important:** It is not possible to recover a password, so if the password is lost or forgotten, you cannot log in to the Technical Support Appliance to change credentials. If you lose or forget your password, contact IBM Support.

- d. Click **Save**.  
The Summary page is displayed.

4. Click **Login**.  
The Summary page is displayed.

**Related concepts:**

“Status information” on page 48

The Technical Support Appliance provides summary information, logs, and reports to enable you to quickly find information about jobs, discovered inventory, and product information.

“Required internet browsers” on page 5

You use a web-based user interface to set up and monitor discovery and transmission.

**Related tasks:**

“Changing your password” on page 49

Change the Technical Support Appliance user password.

---

## Registering the Technical Support Appliance

Registering allows for the activation of the Technical Support Appliance.

### About this task

To register, follow these steps:

### Procedure

1. In the navigation pane, click **Administration > Registration**. The Registration page is displayed.
2. Specify service contact information in the following fields:

**Company name**

The name of the organization that uses the Technical Support Appliance to monitor its systems.

**Contact name**

The name of the person in the organization who is responsible for the Technical Support Appliance.

**Telephone number**

The telephone number where the contact person can be reached. The telephone number must include the area code, exchange numbers, and extension.

**Email** The email address of the contact person.

3. Specify Technical Support Appliance location information in the following fields:

**Country or region**

The country or region where the Technical Support Appliance is located.

**State or province**

The state or province where the Technical Support Appliance is located.

**Postal code**

The postal code of the company.

**City** The city or locality where the Technical Support Appliance is located.

**Street address**

The first line of the Technical Support Appliance location address.

**Telephone number**

The telephone number of the room where the Technical Support Appliance is located. The telephone number must include the area code, exchange numbers, and extension.

**Building, floor, office**

(Optional) The building, floor, and office where the Technical Support Appliance is located.

4. Click **Save** to save the registration information.

---

## Setting the clock

You must set the Technical Support Appliance system time, date, and local time zone during setup.

### About this task

To set the clock, follow these steps:

### Procedure

1. In the navigation pane, click **Administration > Clock**. The Clock page is displayed.
2. Select your local time zone from the **GMT offset** drop-down list.
3. Select the daylight saving time (DST) adjustment from the **DST adjustment** drop-down list.

**Note:** Not all time zones allow DST. If this option is selected for a time zone that does not allow DST, an error message is displayed.

4. Select a method for updating the system clock from the **Select Time Option** drop-down list. Options include synchronizing the system clock with a

Network Time Protocol (NTP) server to update the system clock automatically, or manually configuring the system clock.

- a. If you selected to manually configure the system clock, you must set the system date and time. Enter the date and time information into the **Date** and **Time** fields.
- b. If you selected to synchronize the system clock with the Network Time Protocol (NTP) server to update the system clock automatically, you must then specify the IP addresses and host names for the NTP servers. Type the IP address or host name information for up to two servers in the **NTP server** fields.

**Note:** Make sure that the NTP server is accessible through the network to the Technical Support Appliance.

5. Click **Save** to save the clock information.

## Results

**Note:** Some changes require a restart to take effect. For example, if you set the date or time to an earlier date or time, or changed from manual configuration to NTP server configuration, you are prompted to restart the system.

---

## Configuring network settings

The Technical Support Appliance setup includes configuring network information. Basic network configuration involves configuring the primary Ethernet adapter and other network information. As an alternative, you can configure the Technical Support Appliance to access multiple networks, eliminating the need to set up a specialized anchor server to access those networks.

### About this task

If you want to use basic network settings for the Technical Support Appliance, follow the steps in “Configuring basic network settings.” If you want to configure the Technical Support Appliance to access multiple networks, follow the steps in “Configuring advanced network settings” on page 13.

## Configuring basic network settings

To use basic network settings for the Technical Support Appliance, you must configure the primary Ethernet adapter and other network information.

### Procedure

To configure the network, follow these steps:

1. In the navigation pane, click **Administration > Network**. The Network page is displayed.

#### Identity

2. In the **Hostname** field, specify the unique name for this system on the local network.
3. In the **Domain name suffix** field, specify the name that is used as the domain name for this system on the local network.

#### IP Assignment

4. Select a method for assigning the IP address for this system. Options include dynamically obtaining the IP address from a DHCP server or using a manually configured static IP address.

If you choose to use a manually configured static IP address, you must configure the system IP address on this page.

#### Static IP Configuration

5. If you choose to use a manually configured static IP address, specify the IP information as follows:
  - a. In the **IP address** field, enter the IP address for this system.
  - b. In the **Subnet mask** drop-down list, select the subnet mask to be used by this system.
  - c. In the **Gateway address** field, enter the IP address of the system or router that handles requests out of the current subnet.

#### Name Services

6. Specify a Domain Name System (DNS) server on your network for translating host names into IP addresses.

DNS is a distributed database system for managing host names and their associated Internet Protocol (IP) addresses. Using DNS enables you to use names such as `www.MyCompany.com` to locate a host, rather than using the IP address (`xxx.xxx.xxx.xxx`). A single server might be responsible for knowing the host names and IP addresses for a small subset of a zone, but DNS servers can work together to map all domain names to their IP addresses. DNS servers working together allow computers to communicate across the Internet.

Options include using DNS but obtain server addresses from a DHCP server or using DNS with server addresses that you specify

#### DNS Server Search Order

7. If you choose to use DNS with server addresses you specify, enter up to three IP addresses for Domain Name System (DNS) servers to use when resolving host names. The Technical Support Appliance searches the servers in the order they are displayed.
8. Click **Save** to save the network settings. You are prompted to restart the system.

## Configuring advanced network settings

There might be times when you want to configure the Technical Support Appliance to access multiple networks. For example, configuring the Technical Support Appliance to access multiple networks eliminates the need to set up a specialized anchor server to access those networks. Use the Network (advanced) page to specify these network settings.

To configure advanced network settings, follow these steps:

1. In the navigation pane, click **Administration > Network**.
2. In the lower navigation pane, under **Related links**, click **Advanced network**.  
The Network (advanced) page is displayed.

The Network (advanced) page is divided into the following separate pages:

- Global
- Network Interfaces
- DNS Settings
- Network Routes

To access these individual pages, click the tab for the page you want to display.

**Important:** You must click **Save** before leaving a page to save the changes you made to fields on that page. You are prompted to restart the system for the changes to take effect.

## Global

Use this page to view and change global network settings:

### Identity

Define the identity of this system on the network.

1. In the **Hostname** field, specify the unique name for this system.
2. In the **Domain name suffix** field, specify the name used as the domain name for this system.

## Network Interfaces

Use this page to view and change the network interface settings.

### IP Assignment

Select a method for assigning the IP address for this system. Options include dynamically obtaining the IP address from a DHCP server or using a manually configured static IP address. If you choose to use a manually configured static IP address, you must configure the system IP address on this page.

### Static IP Configuration

If you selected to manually configure a static IP address, specify the IP information for this network interface as follows:

1. In the **IP address** field, specify the IP address for this system.
2. In the **Subnet mask** drop-down list, select the subnet mask to be used by this system.

### Default Gateway Route

Specify whether this network interface provides a route to the default gateway.

### Default Gateway

In the **Gateway address** field, specify the IP address of the default gateway for this system.

## DNS Settings

DNS is a distributed database system for managing host names and their associated Internet Protocol (IP) addresses. Using DNS enables you to use names such as `www.MyCompany.com` to locate a host, rather than using the IP address (`xxx.xxx.xxx.xxx`). A single server might be responsible for knowing the host names and IP addresses for a small subset of a zone, but DNS servers can work together to map all domain names to their IP addresses. DNS servers working together allow computers to communicate across the Internet.

Use this page to view and change the DNS settings.

### Name Services

Specify a domain name system server on your network for translating host names into IP addresses. You can choose from the following options:

- Use DNS, but obtain server addresses from a DHCP server

If you choose this option, you must select the network interface associated with the DHCP server that you want to use.

- Use DNS with server addresses that you specify

If you choose this option, you must specify at least one DNS server on this page.

#### **DHCP Interface**

Select the network interface that is associated with the DHCP server that you want to use.

#### **DNS Server Search Order**

If you choose to use DNS with server addresses you specify, enter up to three IP addresses for Domain Name System (DNS) servers to use when resolving host names. The Technical Support Appliance searches the servers in the order that they are displayed.

#### **Domain Suffix Search Order**

If you choose to use DNS with server addresses you specify, enter up to three domain name suffixes to use when resolving host names. The Technical Support Appliance searches these domain name suffixes in the order they are displayed.

## **Network Routes**

Use this page to view, add, change, or delete static routing entries. The following information is displayed for each network route:

#### **Destination**

Specifies the TCP/IP destination network host or subnet address.

**Mask** Specifies the subnet mask to use as the network mask when adding a route. This is the subnet address for the host portion of the IP address. Network interfaces can use different subnet masks, providing the capability of adding routes by specifying a subnet mask (variable subnet routes). You must specify a subnet mask when adding a route, in 32-bit dotted-decimal notation.

#### **Gateway**

Specifies the TCP/IP gateway address for routing the IP packets. This must be in 32-bit dotted-decimal notation.

#### **Interface**

Select the adapter from the menu. This is the name of the network adapter that is associated with the table entry.

#### **Actions**

Click the **Edit** icon  to edit the route.

Click the **Delete** icon  to delete the route.

Click **Add New Route** to define a new static network route. The Network Route page is displayed.

### **Adding network routes**

You can add static network routes.

## Procedure

To add a network route, follow these steps:

1. In the navigation pane, click **Administration > Network**.
2. In the lower navigation pane, under **Related links**, click **Advanced network**. The Network (advanced) page is displayed.
3. On the Network (advanced) page, click the **Network Routes** tab. The Network Routes page is displayed.
4. On the Network (advanced) - Network Routes page, click **Add New Route**. The Network Route page is displayed.
5. In the **Destination** field, enter the IP address for the TCP/IP destination network host or subnet.
6. In the **Gateway** field, enter the TCP/IP gateway address for routing the information. The address must be in 32-bit dotted decimal notation. For example: xxx.xxx.xxx.xxx.
7. In the **Subnet mask** list, select the subnet mask to use as the network mask for this route.
8. From the **Interface** list, select the network adapter to associate with this route.
9. Click **Save** to save this network route.

---

## Setting up IBM connectivity

Specify the Internet connection information to use when connecting to IBM.

### About this task

To specify the Internet connection information to use when connecting to IBM, follow these steps:

### Procedure

1. In the navigation pane, click **Administration > IBM Connectivity**.
2. In the Access section, select from the following Internet access types:
  - Allow direct SSL connection**  
The system connects to IBM by using a direct connection.
  - Use SSL proxy connection**  
The system connects to IBM by using an SSL proxy connection.
  - Use authenticating SSL proxy connection**  
The system connects to IBM by using an authenticating SSL proxy connection.
3. If you selected an SSL proxy connection, specify the following information for the proxy server.
  - IP address or hostname**  
The IP address or host name of the proxy server.
  - Port** The port number of the proxy server.
4. If you selected an authenticating SSL proxy connection, specify the following information for the proxy server:
  - IP address or host name**  
The IP address or host name of the proxy server.
  - Port** The port number of the proxy server.

**User name**

The user name that the proxy server requires for authentication.

**Password**

The password that is associated with the user name that the proxy server requires for authentication.

**Confirm password**

Enter the password again. The two passwords that you enter are compared to confirm that they match before the password is saved.

5. Click **Save** to save the IBM connection information.
6. Click **Test Connection** to test the specified connection.

**Important:**

- Save the connection settings before testing the connection.
- You must have a working connection to IBM or Technical Support Appliance functions will not work.

**Related concepts:**

“Configuration requirements for connections to IBM Support” on page 5  
The Technical Support Appliance can connect to IBM Support through a direct connection or through a user-supplied proxy that you must configure to allow communication with IBM.

---

## Updating the Technical Support Appliance

Update the Technical Support Appliance to the latest level after you log in for the first time.

**About this task**

To check for updates for the Technical Support Appliance, follow these steps:

**Procedure**

1. In the navigation pane, click **Administration > Update**. The Check for Update page is displayed.
2. Click **Check for Update**. The Update Availability page lists any available updates.
3. To install the updates, click **Perform Update Now**. Upon completion of the update, the Technical Support Appliance is automatically restarted.

---

## Installing an SSL server certificate

The Technical Support Appliance uses a default SSL server certificate to secure data transmission. For added security, you can install a self-signed SSL server certificate that is unique to this Technical Support Appliance, or upload your own SSL server certificate.

**Before you begin**

If you want to upload a custom certificate, you must acquire the certificate. You will need to provide the location of the certificate file, and the password for the certificate.

## About this task

**Note:** When you install a certificate, the Technical Support Appliance is automatically restarted.

To install an SSL server certificate, follow these steps:

### Procedure

1. In the navigation pane, click **Administration > Security**. The Security page is displayed.
2. If you want to install a self-signed server certificate, click **Generate and install a new Self-signed Certificate**. This certificate is unique to this Technical Support Appliance.
3. If you want to install a custom server certificate, follow these steps.
  - a. Enter the password for the certificate in the **Certificate password** field.
  - b. Enter the password again in the **Confirm password** field. The two passwords that you enter are compared to confirm that they match before the password is saved.
  - c. Specify the location of the custom certificate file in the **Custom certificate file** field.
  - d. Click **Upload and install a Custom Certificate**.

### Results

If the server certificate installation completes successfully, the next time you log in to the Technical Support Appliance, you will see the certificate along with a message prompting you to specify whether to trust the certificate.

---

## Setting up user accounts and user groups

Set up user accounts and groups to grant access to Technical Support Appliance functions.

### About this task

Executing any Technical Support Appliance function requires a certain authority level. If an authenticated user attempts to perform a function without the appropriate authority level, an error is displayed and the function is not executed.

In the Technical Support Appliance, authority levels are associated with user groups. Users are assigned membership in one or more user groups, and through those group memberships, users have the authority level to perform particular functions.

The Technical Support Appliance comes with an Administrator user group and an admin user account. The Administrator user group has unrestricted access to all system functions. The admin user account is assigned to the Administrator user group.

### Setting up a user group

Set up user groups to grant access to Technical Support Appliance functions.

## About this task

To set up a user group, follow these steps:

### Procedure

1. In the navigation pane, click **Administration > User Accounts**. The User Accounts and Groups page is displayed.
2. Click the **Groups** tab.
3. Click **Add User Group**. The User Group page is displayed.
4. In the **Group name** field, enter a unique name for this user group.
5. Optional: In the **Description** field, enter a description for this user group.
6. Select the authority level that you want the members of this user group to have.

The Technical Support Appliance defines the following group authority levels:

- **Administrator** – no restrictions
  - **Discovery** – discovery functions only
  - **Visitor** – read access only
7. If you specify the Discovery authority level for this user group, you can optionally select which scope sets this user group has the authority to discover. For more information about scope sets, see “Discovery Scopes and Scope Sets” on page 2.
  8. Click **Save** to save the user group. The User Accounts and Groups page is displayed with the new user group in the list.

## Setting up a user account

Set up user accounts to grant access to Technical Support Appliance functions.

### About this task

To set up a user account, follow these steps:

### Procedure

1. In the navigation pane, click **Administration > User Accounts**. The User Accounts and Groups page is displayed.
2. To define a new user account, click **Add User Account**. The User Account page is displayed.
3. In the **User name** field, enter a name for this user account.
4. Optional: In the **Full name** field, enter a full name for the user of this account.
5. Optional: In the **Description** field, enter a description for this user account.
6. In the **New password** field, enter a password for this user account.

The password must adhere to the following rules:

- Must be at least 8 characters long
- Must contain at least one alphabetic and one non-alphabetic character
- Must not contain the user name
- Must not be the same as any of the previous eight passwords
- Must be changed at least once every 90 days, but must not be changed more than once each day

7. In the **Confirm password** field, enter the password for this user account again. The two passwords that you enter are compared to confirm that they match before the password is saved.

**Note:** The password must be changed at the first login to this user account. This enables you to set up a user account, but prevents you from continuing to use the account.

8. If you want to disable this user account, select the **Account is disabled** check box. Disabling the account enables you to prevent the account from being used without deleting the account.
9. Select the user groups for this user account. The user will have the authority level defined for any groups that you select.
10. Click **Save** to save the user account. The User Accounts and Groups page is displayed with the new user account in the list.

---

## Setting up discovery Scopes

Set up discovery Scopes to specify the IP address, range of IP addresses, or network or subnet to be used during discovery. Discovery Scopes are grouped into discovery Scope Sets.

### About this task

**Tips:** There are some practical considerations for setting up discovery Scopes and Scope Sets.

- The more IP addresses that are in the discovery Scope, the longer the discovery takes. You can modify the discovery size by disabling or enabling Scope Sets or by excluding IP addresses, IP address ranges, or networks or subnets from a Scope within a Scope Set.

To minimize the time that a discovery takes, set up discovery Scopes to target only those elements that you want to discover and disable Scope Sets or exclude IP addresses, IP address ranges, or networks or subnets that you do not want or need to discover.

- Not all elements are equal. For example, a router with dozens of interfaces takes longer to fully discover than a single host.
- Elements can belong to multiple Scopes and Scope Sets. For example, the same IP address can be part of several different Scopes.

The following list contains examples for grouping elements into Scope Sets:

- Group like elements. For example, include all AIX<sup>®</sup> hosts in a Scope Set.
- Group all elements in a location. Because many users manage locations as an entity, specify a Scope Set that includes the entire location.

### Procedure

1. In the navigation pane, click **Discovery Scopes**. The Discovery Scopes page is displayed.
2. To define a new discovery Scope Set, click **Add New Scope Set**. The Discovery Scope Set page is displayed.
  - a. For Describe Scope Set, in the **Scope set name** field, enter a unique Scope Set name.
  - b. Click **Save**. The new Scope Set is created and the **Discovery Scopes** page is displayed.

3. To add a Scope to the new Scope Set, in the Select Discovery Option pane, specify one of the following options:
  - Single IP address or Host  
For **Describe Address or Host**, enter the IP address.
  - Range of IP addresses  
For **Describe Address Range**, enter the starting IP address, ending IP address, and optionally, a description in the fields provided.
  - Network or Subnet  
For **Describe Network or Subnet**, enter the IP address, mask, and optionally, a description in the fields provided.
4. If you want to exclude hosts, IP addresses, or subnets from the discovery, click **Add Exclusion** and follow these steps:
  - a. Select Host, Range, or Subnet.
  - b. Specify the IP address, range of IP addresses, or subnet that you want to exclude from the discovery.
  - c. Optional: Specify a description for the IP address, range of IP addresses or subnet that you are excluding from the discovery.  
  
**Note:** You cannot reuse an IP address, range of IP addresses, subnet, or description in any Scopes or exclusions in a Scope Set.
  - d. To add more exclusions, click **Add Exclusion** and follow the previous steps to define more exclusions.
5. Click **Save** to save the Scope and exclusions. The Discovery Scope Set page is displayed with the new Scope in the list.
6. To add more Scopes to this Scope Set, click **Add New Scope** and follow the previous steps to define more Scopes.

**Related concepts:**

“Discovery Scopes and Scope Sets” on page 2

Discovery Scopes identify the resources that you want the Technical Support Appliance to discover. Discovery Scopes are grouped into discovery Scope Sets.

---

## Setting up discovery credentials

Set up discovery credentials to provide access control for the discovery process.

### About this task

To set up discovery credentials, follow these steps:

### Procedure

1. In the navigation pane, click **Discovery Credentials**. The Discovery Credentials page is displayed.
2. To create a credential, click **Add New Credentials**. The New Discovery Credentials page is displayed.
  - a. In the **Name** field, type an identifying name for the credential.
  - b. In the Credential Type drop-down list, select the type of credential that you want to create.
  - c. In the Enter Access Information pane, specify the information for the credential type you selected:

The information that is required depends on the credential type. For information about the access information that is required for each type of credential, see “Credential and software requirements for the discovery environment” on page 6.

**Important:** The access information that you specify must match the access information for the discovery target resource. If you change access information about the target resource, be sure to also change the associated Technical Support Appliance access information.

**Tip:** The Discovery Credentials page displays the last time that the password was changed. If you regularly change the password on the target resource, you can use this information to make sure that you also change the password on the Technical Support Appliance to match the new password for the target resource. For information about displaying the discovery credentials, see “Displaying credentials” on page 37.

- d. In the Select Scope Set Restriction pane, specify whether to use the access information across all components of the entire discovery scope or to limit the access information to a selected scope.

**Tip:** Creating discovery credentials that are restricted to a specific scope set can improve performance by reducing the number of credentials that are attempted for resources that are being discovered. For information about creating discovery scope sets, see “Setting up discovery Scopes” on page 20.

- e. If you choose to limit the access to a scope set that you specify, select the scope set from the **Scope set name** drop-down list in the Restrict To Selected Scope Set pane. The credential is used only when discovering with the selected scope. When discovering with a different scope, the credential is not used. This method prevents invalid login attempts that can result in the user being locked out of the account.
- f. If your credential type is **Computer System** or **Computer System (Windows)**, you can verify whether the credentials are correct. To test these credentials, enter an IP address or a host name for the computer system against which you want to test the credentials and click **Test**.

**Note:** For the Computer System credential type, only SSH and Telnet based authentication systems are supported.

- g. Click **Save**. The new credential is displayed in the Discovery Credentials page.
3. To change the order in which a credential is used by the Technical Support Appliance to access a resource, click either the **Up arrow** icon or the **Down arrow** icon beside the credential to move it up or down in the list. For information about how the order is used, see “Discovery credentials” on page 2. The Discovery Credentials page list is displayed again with the new order.

**Related concepts:**

“Discovery credentials” on page 2

Discovery credentials are a collection of user names, passwords, and Simple Network Management Protocol (SNMP) community strings that the Technical Support Appliance uses to access resources during the discovery.

“Credential and software requirements for the discovery environment” on page 6

In order to discover endpoints or resources in your environment, the Technical Support Appliance must have access to those resources. It is recommended that you create a service account on each resource that is specifically for the Technical Support Appliance to use when accessing that resource.

**Related tasks:**

“Modifying credentials” on page 39

You can modify existing credentials to provide access control for the discovery process.

## Configuring key pair authentication

You must configure discovery credentials on the Technical Support Appliance to enable discovery on target computer systems. You can configure credentials that use user name and password authentication or OpenSSH Version 2 key-pair authentication. The advantage of using key-pair authentication is that you do not have to maintain passwords in the Technical Support Appliance for service accounts that exist on the target computer systems.

### Before you begin

Before you configure discovery credentials that use key-pair authentication, ensure the following:

- OpenSSH is installed on the target computer systems
- The SSH daemon is running on the target computer systems
- The service account is created on the target computer systems and has the necessary authorizations for the relevant platform
- No firewalls are blocking access from the Technical Support Appliance to the target computer systems on port 22

For more information about SSH, see the following sources:

**OpenSSH**

<http://www.openssh.org/manual.html>

**SSH.com**

<http://www.ssh.com/index.php/support-overview/product-documentation.html>

### About this task

Configuring discovery credentials that use key-pair authentication requires that you perform the following tasks:

- Generate the key pair
- Download the generated public key
- Deploy the public key to the target computer systems that you want to discover
- Create the discovery credential

## Procedure

### Generate the key pair

1. In the navigation pane, click **Administration > Security**. The Security page is displayed.
2. Enter a passphrase in the **Passphrase** field.

**Important:** The passphrase must be at least eight characters long and contain at least one numeric and one alphabetic character. A good passphrase is 10 - 30 characters long and consists of both numeric characters and random upper and lowercase alphabetic characters.

3. Enter the passphrase again in the **Confirm Passphrase** field. The two passphrases that you enter are compared to confirm that they match before the passphrase is saved.
4. Save the passphrase in a secure location for use in later configuration steps.
5. Click **Generate SSH Server Public/Private Key Pair**. A message that the key pair has been generated along with a **Download SSH Server Public Key** button is displayed in the SSH Server Key Status pane.

### Download the generated public key

6. Click **Download SSH Server Public Key** to download the public key on the system that you are using to sign on to the Technical Support Appliance. This is the key that you deploy on the target computer systems.

### Deploy the public key to the target systems

7. Use any available process or utility to deploy the public key to the target computer systems.

**Note:** Utilities exist in most SSH implementations to assist with deploying public keys. For example, OpenSSH includes an `ssh-copy-id` utility that you can use to deploy the public key to the target computer systems.

If the `ssh-copy-id` utility is available on the system that you are using to sign on to the Technical Support Appliance, you can deploy the public key to a target system by running the following command:

```
ssh-copy-id -i id_rsa.pub serviceaccount@remotehost
```

If the `ssh-copy-id` utility is not available, insert the contents of the public key file (`id_rsa.pub`) into the `$HOME/.ssh/authorized_keys` file for the service account on each target computer system where you want to use key-pair authentication.

### Create the discovery credential

8. In the navigation pane, click **Discovery Credentials**. The Discovery Credentials page is displayed.
9. Click **Add New Credentials**. The New Discovery Credentials page is displayed.
  - a. In the **Name** field, type an identifying name for the credential.
  - b. In the Credential Type drop-down list, select **Computer System**.
  - c. In the Enter Access Information pane, specify the following information:

#### User name

The user name for the service account on the target computer system.

#### Password

The passphrase you specified when generating the public/private key pair.

### Confirm password

Enter the passphrase again. The two passphrases that you enter are compared to confirm that they match before the passphrase is saved.

### Authentication type

Select Public Key Infrastructure (PKI).

- d. Click **Save**. The new credential is displayed in the Discovery Credentials page.

The Technical Support Appliance can now run discoveries against the target computer systems that have this service account configured and the public key installed, and login to the operating system using OpenSSH Version 2 key-based authentication.

---

## Setting up discovery anchors

Set up discovery anchor servers to enable discovery by providing access to resources that are protected by a firewall.

### About this task

To set up an anchor server, follow these steps:

### Procedure

1. In the navigation pane, click **Discovery Anchors**. The Discovery Anchors page is displayed.
2. If the default anchor port number is in use on the anchor server, you can change the anchor port number. To change the anchor port number, click **Edit Port**. The Anchor Port page is displayed.
  - a. Specify the port number that you want the Technical Support Appliance to use for all defined anchor servers.
  - b. Click **Save**. The port number is displayed in the Discovery Anchors page.
3. In the Discovery Anchors page, click **Add New Anchor**. The Discovery Anchor page is displayed.
  - a. In the **IP address** field, specify the IP address or host name for the server you want to use as an anchor.

**Note:** The anchor must be in the same network section as the resources that you want to discover.

- b. In the Select Scope Set Restriction pane, specify whether to use the anchor server across all defined discovery scopes or limit the anchor server to a scope that you specify.

**Note:** The anchor server scope should be restricted to the systems in that network section.

- c. If you chose to limit the anchor server to a specified scope, select the scope set for this anchor server in the Describe Scope Set Restriction pane.
- d. Click **Save**. The new anchor is displayed in the Discovery Anchors page.

---

## Modifying the discovery schedule

The Technical Support Appliance provides a default schedule for the discovery process to run at specified times. You can modify this schedule according to your needs.

### About this task

To modify the discovery schedule, follow these steps:

### Procedure

1. In the navigation pane, click **Discovery Schedule**. The Discovery Schedule page is displayed.  
The Schedule pane displays the next scheduled run and the scheduled run times. The History pane displays the status and more details of the currently running and previous discovery jobs.
2. Click **Edit Schedule**. The Discovery Schedule page is displayed.
  - a. In the Enable Schedule pane, select whether you want to enable or disable scheduled discoveries.
  - b. Use the **At hour** and **At minute** drop-down lists to select a new time.
  - c. For the **On days** field, select the appropriate check box to select different or more days of the week.
3. Click **Save**. The Discovery Schedule page is displayed again, with the new schedule shown.

### Related concepts:

“Discovery schedule” on page 3

Discoveries run on scheduled days and times to ensure that discovered data is always current and accurate. The Technical Support Appliance has a default discovery schedule that you can modify for your needs. You can also view details, history, and the state of the last discovery that was run.

---

## Running the discovery

You can run a discovery on demand, rather than wait for the next scheduled discovery. You can run a discovery on all defined discovery scopes or on specific discovery scopes.

### Procedure

To run a discovery on all defined scopes, follow these steps:

1. In the navigation pane, click **Discovery Schedule**. The Discovery Schedule page is displayed.
2. Click **Run Discovery Now**. The History section is updated indicating that the discovery is running.

**Note:** When you are running a discovery that requires anchors, ensure that each anchor is included in the discovery scope. For example, to discover a target that is in a scope set assigned to an anchor, both the anchor and the scope set must be included in the discovery run. For information, see “Setting up discovery Scopes” on page 20.

## Running the discovery on specific scope sets

You can run a discovery on a specific scope set.

## Procedure

To run a discovery on a specific scope set, follow these steps:

1. In the navigation pane, click **Discovery Scopes**. The Discovery Scopes page is displayed. This page displays a list of all scope sets that are defined for this Technical Support Appliance.
2. To run a discovery on a specific scope set, click the **Run** icon for that scope set.

## Running discovery on specific scopes

You can run a discovery on a specific scope.

### Procedure

To run a discovery on a specific scope, follow these steps:

1. In the navigation pane, click **Discovery Scopes**. The Discovery Scopes page is displayed.
2. Click the scope set that contains the scope on which you want to run a discovery. The Discovery Scope Set page is displayed. This page displays all the scopes that are defined for that scope set.
3. To run a discovery on a specific scope, click the **Run** icon for that scope.

---

## Modifying the transmission schedule

The Technical Support Appliance provides a default schedule for the transmission process to run at specified times. You can modify this schedule according to your needs.

### About this task

To modify the transmission schedule, follow these steps.

### Procedure

1. In the navigation pane, click **Transmission Schedule**. The Transmission Schedule page is displayed.

The Schedule pane displays the next scheduled run and the scheduled run times. The History pane displays the status and additional details of the currently running and previous transmission jobs.
2. Click **Edit Schedule**. The Transmission Schedule page is displayed.
  - a. Use the **At hour** and **At minute** drop-down lists to select a new time.
  - b. For the **On days** field, select the appropriate check box to select different or additional days of the week.
3. Click **Save**. The Transmission Schedule page is displayed again, with the new schedule shown.

**Related concepts:**

“Transmission schedule” on page 3

Discovered data is securely packaged and transmitted to IBM Support on regularly scheduled days and times to ensure that IBM has the most current and accurate information. A default transmission schedule, that you can modify for your needs, is provided. You can also run transmissions on demand.

---

## Running the transmission

You can run a transmission on demand, rather than wait for the next scheduled transmission.

### About this task

To run the transmission immediately, follow these steps:

### Procedure

1. In the navigation pane, click **Transmission Schedule**. The Transmission Schedule page is displayed.
2. Click **Run Transmission Now**. The History section is updated indicating that the transmission is running.

**Tip:** To save the results of the data collection, click **Download Last Collection** and specify a location for the results.

Depending on the amount of data, the save operation might take some time.

---

## Chapter 4. Using the Technical Support Appliance

After the Technical Support Appliance setup is complete, you can use various administration features to manage discovery, transmission, and jobs.

---

### User accounts and user groups

You can use user accounts and user groups to grant access to Technical Support Appliance functions.

#### Displaying user accounts and user groups

You can display the existing user accounts and user groups.

##### About this task

To display existing user accounts and user groups, follow these steps:

##### Procedure

1. In the navigation pane, click **Administration > User Accounts**. The User Accounts and Groups page is displayed.
2. To display the existing user accounts, click the **Accounts** tab. The User Accounts table displays the user accounts.

**Tip:** To view details for a specific user account, click the name of the user account. The General section displays the user name, full name, and description that is associated with the selected user account. The Member Of section displays the user groups to which this user account belongs.

3. To display the existing user groups, click the **Groups** tab. The User Groups table displays the user groups.

**Tip:** To view details for a specific user group, click the name of the user group. The General section displays the name and authority level that is associated with the user group. The Scope restrictions section displays the scope sets that the selected user group can discover. The Members section displays the user accounts that are associated with this user group.

#### Adding user accounts and user groups

You can add user accounts and groups to control access to Technical Support Appliance functions.

##### Related concepts:

“Discovery Scopes and Scope Sets” on page 2

Discovery Scopes identify the resources that you want the Technical Support Appliance to discover. Discovery Scopes are grouped into discovery Scope Sets.

##### Adding a user group

You can add user groups to control access to Technical Support Appliance functions.

##### About this task

To add a user group, follow these steps:

## Procedure

1. In the navigation pane, click **Administration > User Accounts**. The User Accounts and Groups page is displayed.
2. Click the **Groups** tab.
3. Click **Add User Group**. The User Group page is displayed.
4. In the **Group name** field, enter a unique name for this user group.
5. Optional: In the **Description** field, enter a description for this user group.
6. Select the authority level that you want the members of this user group to have.

The Technical Support Appliance defines the following group authority levels:

- **Administrator** – no restrictions
  - **Discovery** – discovery functions only
  - **Visitor** – read access only
7. If you specify the Discovery authority level for this user group, you can optionally select which scope sets this user group has the authority to discover. For more information about scope sets, see “Discovery Scopes and Scope Sets” on page 2.
  8. Click **Save** to save the user group. The User Accounts and Groups page is displayed with the new user group in the list.

## Adding a user account

You can add user accounts to control access to Technical Support Appliance functions.

### About this task

To add a user account, follow these steps:

## Procedure

1. In the navigation pane, click **Administration > User Accounts**. The User Accounts and Groups page is displayed.
2. To define a new user account, click **Add User Account**. The User Account page is displayed.
3. In the **User name** field, enter a name for this user account.
4. Optional: In the **Full name** field, enter a full name for the user of this account.
5. Optional: In the **Description** field, enter a description for this user account.
6. In the **New password** field, enter a password for this user account.

The password must adhere to the following rules:

- Must be at least 8 characters long
  - Must contain at least one alphabetic and one non-alphabetic character
  - Must not contain the user name
  - Must not be the same as any of the previous eight passwords
  - Must be changed at least once every 90 days, but must not be changed more than once each day
7. In the **Confirm password** field, enter the password for this user account again. The two passwords that you enter are compared to confirm that they match before the password is saved.

**Note:** The password must be changed at the first login to this user account. This enables you to set up a user account, but prevents you from continuing to use the account.

8. If you want to disable this user account, select the **Account is disabled** check box. Disabling the account enables you to prevent the account from being used without deleting the account.
9. Select the user groups for this user account. The user will have the authority level defined for any groups that you select.
10. Click **Save** to save the user account. The User Accounts and Groups page is displayed with the new user account in the list.

## Modifying user accounts and user groups

You can modify existing user accounts and user groups.

### Modifying user accounts

You can modify existing user accounts.

#### About this task

To modify a user account, follow these steps:

#### Procedure

1. In the navigation pane, click **Administration > User Accounts**. The User Accounts and Groups page is displayed.
2. Click the **Accounts** tab, and then click the **Edit** icon beside the user account. The User Account page is displayed.
3. In the General pane, you can change the basic information for this user account.
4. In the Enter Password pane, you can change the password and password administration information. You can also disable this user account.

The password must adhere to the following rules:

- Must be at least 8 characters long
- Must contain at least one alphabetic and one non-alphabetic character
- Must not contain the user name
- Must not be the same as any of the previous eight passwords
- Must be changed at least once every 90 days, but must not be changed more than once each day

**Note:** The password must be changed at the first login to this user account. This enables you to set up a user account, but prevents you from continuing to use the account.

5. If you want to disable this user account, select **Account is disabled**. Disabling the account enables you to prevent the account from being used without deleting the account. For information about deleting a user account, see “Deleting user accounts and user groups” on page 32.
6. In the Member Of pane, you can change the user groups to which this user account belongs.
7. Click **Save** to save your changes. The changed information is displayed in the User Accounts and Groups page.

### Modifying user groups

You can modify existing user groups.

## About this task

To modify a user group, follow these steps:

### Procedure

1. In the navigation pane, click **Administration > User Accounts**. The User Accounts and Groups page is displayed.
2. Click the **Groups** tab, and then click the **Edit** icon . beside the user group. The User Group page is displayed.
3. In the General pane, you can change the basic information for this user group.
4. In the Member Authority Level pane, you can change whether this user group has Administrator, Discovery, or Read authority.
5. If you specified Discovery authority level in the Restrict To Selected Scope Sets pane, you can change the scope sets that this user group has the authority to discover.
6. Click **Save** to save your changes. The changed information is displayed in the User Accounts and Groups page.

## Deleting user accounts and user groups

You can delete existing user accounts and user groups.

### Deleting user accounts

You can delete existing user accounts.

## About this task

**Note:** The admin user account cannot be deleted.

To delete a user account, follow these steps:

### Procedure

1. In the navigation pane, click **Administration > User Accounts**. The User Accounts and Groups page is displayed.
2. Click the **Accounts** tab, and then click the Delete icon . next the user account that you want to delete.
3. Click **OK** to confirm that you want to delete the user account.

### Deleting user groups

You can delete existing user groups.

## About this task

**Note:** The Administrator user group cannot be deleted.

To delete a user group, follow these steps:

### Procedure

1. Click **Administration > User Accounts**. The User Accounts and Groups page is displayed.
2. Click the **Groups** tab, and then click the Delete icon . next to the user group that you want to delete.
3. Click **OK** to confirm that you want to delete the user group.

---

## Discovery Scopes

A discovery sScope specifies the IP address, range of IP addresses, or network to be used to discover resources. Discovery Scopes are grouped into discovery Scope Sets.

### Displaying discovery Scopes and Scope Sets

You can display the existing discovery Scopes and Scope Sets.

#### About this task

To display the existing discovery Scope Sets, click **Discovery Scopes** in the navigation pane. The Discovery Scopes page is displayed. The Scope Sets pane contains a list of the Scope Sets.

To display the Scopes that a Scope Set contains, click the Scope Set. The Discovery Scope Set page is displayed. The Scopes pane displays details about the Scopes in the Scope Set.

### Adding discovery Scopes

You can add a Scope Set and a new Scope to that set, add a Scope to an existing Scope Set or move Scopes to other Scope Sets. To add a Scope, specify a valid IP address, a range of IP addresses, a network, or subnet.

#### About this task

**Tips:** There are some practical considerations for setting up discovery Scopes and Scope Sets.

- The more IP addresses that are in the discovery Scope, the longer the discovery takes. You can modify the discovery size by disabling or enabling Scope Sets or by excluding IP addresses, IP address ranges, or networks or subnets from a Scope within a Scope Set.

To minimize the time that a discovery takes, set up discovery Scopes to target only those elements that you want to discover and disable Scope Sets or exclude IP addresses, IP address ranges, or networks or subnets that you do not want or need to discover.

- Not all elements are equal. For example, a router with dozens of interfaces takes longer to fully discover than a single host.
- Elements can belong to multiple Scopes and Scope Sets. For example, the same IP address can be part of several different Scopes.

The following list contains examples for grouping elements into Scope Sets:

- Group like elements. For example, include all AIX hosts in a Scope Set.
- Group all elements in a location. Because many users manage locations as an entity, specify a Scope Set that includes the entire location.

To add a Scope Set and Scope, follow these steps:

#### Procedure

1. In the navigation pane, click **Discovery Scopes**. The Discovery Scopes page is displayed.
2. To define a new discovery Scope Set, click **Add New Scope Set**. The Discovery Scope Set page is displayed.

- a. For Describe Scope Set, in the **Scope set name** field, enter a unique Scope Set name.
  - b. Click **Save**. The new Scope Set is created and the **Discovery Scopes** page is displayed.
3. To add a Scope to the new Scope Set, in the Select Discovery Option pane, specify one of the following options:
    - Single IP address or Host  
For **Describe Address or Host**, enter the IP address.
    - Range of IP addresses  
For **Describe Address Range**, enter the starting IP address, ending IP address, and optionally, a description in the fields provided.
    - Network or Subnet  
For **Describe Network or Subnet**, enter the IP address, mask, and optionally, a description in the fields provided.
  4. If you want to exclude hosts, IP addresses, or subnets from the discovery, click **Add Exclusion** and follow these steps:
    - a. Select Host, Range, or Subnet.
    - b. Specify the IP address, range of IP addresses, or subnet that you want to exclude from the discovery.
    - c. Optional: Specify a description for the IP address, range of IP addresses or subnet that you are excluding from the discovery.  
  
**Note:** You cannot reuse an IP address, range of IP addresses, subnet, or description in any Scopes or exclusions in a Scope Set.
    - d. To add more exclusions, click **Add Exclusion** and follow the previous steps to define more exclusions.
  5. Click **Save** to save the Scope and exclusions. The Discovery Scope Set page is displayed with the new Scope in the list.
  6. To add more Scopes to this Scope Set, click **Add New Scope** and follow the previous steps to define more Scopes.

## Adding a discovery Scope to an existing Scope Set

You can add a Scope to an existing scope set.

### Procedure

To add a Scope to an existing Scope Set, follow these steps:

1. In the navigation pane, click **Discovery Scopes**. The Discovery Scopes page is displayed.
2. In the Scope Sets pane, click the Scope Set to which you want to add a Scope. The Discovery Scope Set page is displayed.
3. Click **Add New Scope**. The Discovery Scopes page is displayed.
4. In the Select Discovery Option pane, specify one of the following options.
  - Single IP address or Host  
For **Describe Address or Host**, enter the IP address.
  - Range of IP addresses  
For **Describe Address Range**, enter the starting IP address, ending IP address, and a description in the fields provided.
  - Network or Subnet

For **Describe Network or Subnet**, enter the IP address, mask, and a description in the fields provided.

5. If you want to exclude hosts, IP addresses, or subnets from the discovery, click **Add Exclusion** and follow these steps:
  - a. Select Host, Range, or Subnet.
  - b. Specify the IP address, range of IP addresses, or subnet that you want to exclude from the discovery.
  - c. Optional: Specify a description for the IP address, range of IP addresses or subnet that you are excluding from the discovery.

**Note:** You cannot reuse an IP address, range of IP addresses, subnet, or description in any Scopes or exclusions in a Scope Set.

- d. To add more exclusions, click **Add Exclusion** and follow the previous steps to define more exclusions.
6. Click **Save** to save the Scope and the exclusions. The Discovery Scope Set page is displayed with the new Scope in the list.

## Moving Scopes from one Scope Set to another Scope Set

You can move one or more Scopes from one Scope Set to another Scope Set.

### Procedure

To move Scopes from one Scope Set to another Scope Set, follow these steps:

1. In the navigation pane, click **Discovery Scopes**. The Discovery Scopes page is displayed.
2. In the **Scope Sets** pane, click to select a Scope Set from which you want to move Scopes. The Discovery Scope Set page is displayed.
3. Click **Move Scopes**. The Move Scopes from one set to another page is displayed.
4. Select the Scopes that you want to move from the **Scopes** list. You can select one or more Scopes here.
5. Select the Scope Set, from the **Destination Scope Set** list, to which you want to move the Scopes.
6. Click **Move**.

## Modifying a discovery Scope Set

You can modify an existing discovery Scope Set to change the settings for the Scope Set.

### About this task

To modify an existing discovery Scope Set, follow these steps.

### Procedure

1. In the navigation pane, click **Discovery Scopes**. The Discovery Scopes page is displayed.
2. To edit the Scope Set, click the **Edit** icon . beside the Scope Set. The Discovery Scope Set page is displayed. You can edit the Scope Set by adding a Scope, moving a Scope to another Scope Set, or by deleting a Scope.
  - To add a Scope, follow these steps:
    - a. Click **Add New Scope**.

- b. In the Select Discovery Option pane, specify one of the following options:
    - Single IP address / host  
For Describe Address or Host, type the IP address and a description in the fields provided.
    - Range of IP addresses  
For Describe Address Range, type the starting IP address, ending IP address, and a description in the fields provided.
    - Network or Subnet  
For Describe Network or Subnet, type the IP address, mask, and a description in the fields provided.
  - c. If you want to exclude hosts, IP addresses, or subnets from the discovery, click **Add Exclusion** and follow these steps:
    - 1) Select Host, Range, or Subnet.
    - 2) Specify the IP address, range of IP addresses, or subnet that you want to exclude from the discovery.
    - 3) To add more exclusions, click **Add Exclusion** and follow the previous steps to define more exclusions.
  - d. Click **Save** to save the Scope and exclusions. The Discovery Scope Set page is displayed with the new Scope in the list.
- To move a Scope to another Scope Set, follow these steps:
    - a. Click **Move Scopes**.
    - b. On the Move Scopes from one set to another page, select the Scopes that you want to move from the **Scopes** list.
    - c. Select the Scope Set, from the **Destination Scope Set** list, to which you want to move the Scopes.
    - d. Click **Move**.
  - To delete a Scope, follow these steps:
    - a. Click the **Delete** icon . beside the Scope that you want to delete.
    - b. Click **OK** to confirm that you want to delete the discovery Scope.

## Deleting discovery Scopes

You can delete existing discovery Scopes within a Scope Set, or you can delete entire Scope Sets.

### About this task

#### Procedure

To delete a discovery Scope, follow these steps:

1. In the navigation pane, click **Discovery Scopes**. The Discovery Scopes page is displayed.
2. Edit the Scope Set that contains the discovery Scope that you want to delete by clicking the **Edit** icon . beside the Scope Set. The Discovery Scope Set page is displayed.
3. Click the **Delete** icon . beside the Scope that you want to delete.
4. Click **OK** to confirm that you want to delete the discovery Scope.

### Deleting discovery Scope Sets

You can delete existing discovery Scope Sets.

## Procedure

**Note:** Before you can delete a Scope Set, you must delete all credentials, anchors and gateways associated with the Scope Set or remove their associations with this Scope Set.

To delete a discovery Scope Set, follow these steps:

1. In the navigation pane, click **Discovery Scopes**. The Discovery Scopes page is displayed.
2. Click the **Delete** icon beside the Scope Set that you want to delete.
3. Click **OK** to confirm that you want to delete the discovery Scope Set.

---

## Discovery credentials

Discovery credentials are the user names, passwords, and SNMP community strings that the Technical Support Appliance uses to access resources during discovery.

### Displaying credentials

The discovery process requires credentials, such as user IDs and passwords, to access resources.

#### About this task

**Important:** The access information that you specify must match the access information for the discovery target resource. If you change access information, such as a password, on the target resource, be sure to also change the associated Technical Support Appliance access information.

You can display the existing credentials, if any, by clicking **Discovery Credentials** in the navigation pane. The Discovery Credentials page is displayed.

### Viewing credential details

You can view detailed information about a specific discovery credential.

#### About this task

To view the credential details, follow these steps:

#### Procedure

1. In the navigation pane, click **Discovery Credentials**. The Discovery Credentials page is displayed with all the existing credentials listed.
2. To view details for a specific credential, click the name of the credential. The Discovery Credentials page is displayed with information for the selected credential. The General section displays the name and type of credential. The Properties section displays the name and value of various properties of the credential.

#### Related tasks:

“Modifying credentials” on page 39

You can modify existing credentials to provide access control for the discovery process.

### Adding credentials

Add credentials to provide access control for the discovery process.

## About this task

To add credentials, follow these steps:

### Procedure

1. In the navigation pane, click **Discovery Credentials**. The Discovery Credentials page is displayed.
2. To create a credential, click **Add New Credentials**. The New Discovery Credentials page is displayed.
  - a. In the **Name** field, type an identifying name for the credential.
  - b. In the Credential Type drop-down list, select the type of credential that you want to create.
  - c. In the Enter Access Information pane, specify the information for the credential type you selected:

The information that is required depends on the credential type. For information about the access information that is required for each type of credential, see “Credential and software requirements for the discovery environment” on page 6.

**Important:** The access information that you specify must match the access information for the discovery target resource. If you change access information about the target resource, be sure to also change the associated Technical Support Appliance access information.

**Tip:** The Discovery Credentials page displays the last time that the password was changed. If you regularly change the password on the target resource, you can use this information to make sure that you also change the password on the Technical Support Appliance to match the new password for the target resource. For information about displaying the discovery credentials, see “Displaying credentials” on page 37.

- d. In the Select Scope Set Restriction pane, specify whether to use the access information across all components of the entire discovery scope or to limit the access information to a selected scope.

**Tip:** Creating discovery credentials that are restricted to a specific scope set can improve performance by reducing the number of credentials that are attempted for resources that are being discovered. For information about creating discovery scope sets, see “Setting up discovery Scopes” on page 20.

- e. If you choose to limit the access to a scope set that you specify, select the scope set from the **Scope set name** drop-down list in the Restrict To Selected Scope Set pane. The credential is used only when discovering with the selected scope. When discovering with a different scope, the credential is not used. This method prevents invalid login attempts that can result in the user being locked out of the account.
- f. If your credential type is **Computer System** or **Computer System (Windows)**, you can verify whether the credentials are correct. To test these credentials, enter an IP address or a host name for the computer system against which you want to test the credentials and click **Test**.

**Note:** For the Computer System credential type, only SSH and Telnet based authentication systems are supported.

- g. Click **Save**. The new credential is displayed in the Discovery Credentials page.

3. To change the order in which a credential is used by the Technical Support Appliance to access a resource, click either the **Up arrow** icon or the **Down arrow** icon beside the credential to move it up or down in the list. For information about how the order is used, see “Discovery credentials” on page 2. The Discovery Credentials page list is displayed again with the new order.

## Modifying credentials

You can modify existing credentials to provide access control for the discovery process.

### About this task

To modify credentials, follow these steps:

### Procedure

1. In the navigation pane, click **Discovery Credentials**. The Discovery Credentials page is displayed with all the existing credentials listed.
2. Edit the credential by clicking the **Edit** icon beside the credential. The Edit Discovery Credentials page is displayed.
  - a. In the Modify Access Information pane, you can change the access information for this credential.

**Important:** The access information that you specify must match the access information for the discovery target resource. If you change access information about the target resource, be sure to also change the associated Technical Support Appliance access information.

**Tip:** The Discovery Credentials page displays the last time that the password was changed. If you regularly change the password on the target resource, you can use this information to make sure that you also change the password on the Technical Support Appliance to match the new password for the target resource. For information about displaying the discovery credentials, see “Displaying credentials” on page 37.

- b. In the Select Scope Set Restriction pane, specify whether to use the access information across all components of the entire discovery scope or to limit the access information to a selected scope.

**Tip:** Creating discovery credentials that are restricted to a specific scope set can improve performance by reducing the number of credentials that are attempted for resources being discovered.

- c. If you choose to limit the access to a scope set that you specify, select the scope set from the **Scope set name** drop-down list in the Restrict To Selected Scope Set pane. The credential is used only when discovering using the selected scope. When discovering using a different scope, the credential is not used. This method prevents invalid login attempts that can result in the user being locked out of the account.
- d. If your credential type is **Computer System** or **Computer System (Windows)**, you can verify whether the credentials are correct. To test these credentials, enter an IP address or a host name for the computer system against which you want to test the credentials and click **Test**.
- e. Click **Save**. The changed credential is displayed in the Discovery Credentials page.

3. To change the priority order in which a credential is used by the Technical Support Appliance to access a resource, click either the **Up arrow** icon or the **Down arrow** icon beside the credential to move it up or down in the list. For information about how the order is used, see “Discovery credentials” on page 2. The Discovery Credentials page list is displayed again with the new order.

**Related concepts:**

“Discovery credentials” on page 2

Discovery credentials are a collection of user names, passwords, and Simple Network Management Protocol (SNMP) community strings that the Technical Support Appliance uses to access resources during the discovery.

“Credential and software requirements for the discovery environment” on page 6

In order to discover endpoints or resources in your environment, the Technical Support Appliance must have access to those resources. It is recommended that you create a service account on each resource that is specifically for the Technical Support Appliance to use when accessing that resource.

## Deleting credentials

You can delete credentials that the Technical Support Appliance uses when accessing your resources.

### About this task

To delete a credential, follow these steps:

### Procedure

1. In the navigation pane, click **Discovery Credentials**. The Discovery Credentials page is displayed.
2. Click the **Delete** icon beside the credential that you want to delete.
3. Click **OK** to confirm that you want to delete the credential.

---

## Discovery anchors

A discovery anchor is a proxy server that has access to computer hosts or network devices that are protected by a firewall and thus cannot be discovered directly. The discovery anchor enables the discovery by communicating with the resources behind the firewall.

## Displaying anchors

You can display the defined discovery anchor servers.

### About this task

To display the existing anchor servers, click **Discovery Anchors** in the navigation pane. The Discovery Anchors page is displayed.

## Editing the anchor port

The Technical Support Appliance uses port 8497 on the anchor server. If this port is being used by another application that is running on the anchor server, you can change the port number.

### About this task

To change the anchor port number, follow these steps:

## Procedure

1. In the navigation pane, click **Discovery Anchors**. The Discovery Anchors page is displayed.
2. In the Discovery Anchors page, click **Edit Port**. The Anchor Port page is displayed.
3. Specify the port number that you want the Technical Support Appliance to use for the anchor server process. All anchor servers must use the same port number.

## Adding anchors

You can add discovery anchors to provide access to resources that are protected by a firewall.

### About this task

To add anchors, follow these steps:

## Procedure

1. In the navigation pane, click **Discovery Anchors**. The Discovery Anchors page is displayed.
2. If the default anchor port number is in use on the anchor server, you can change the anchor port number. To change the anchor port number, click **Edit Port**. The Anchor Port page is displayed.
  - a. Specify the port number that you want the Technical Support Appliance to use for all defined anchor servers.
  - b. Click **Save**. The port number is displayed in the Discovery Anchors page.
3. In the Discovery Anchors page, click **Add New Anchor**. The Discovery Anchor page is displayed.
  - a. In the **IP address** field, specify the IP address or host name for the server you want to use as an anchor.

**Note:** The anchor must be in the same network section as the resources that you want to discover.

- b. In the Select Scope Set Restriction pane, specify whether to use the anchor server across all defined discovery scopes or limit the anchor server to a scope that you specify.

**Note:** The anchor server scope should be restricted to the systems in that network section.

- c. If you chose to limit the anchor server to a specified scope, select the scope set for this anchor server in the Describe Scope Set Restriction pane.
- d. Click **Save**. The new anchor is displayed in the Discovery Anchors page.

## Modifying anchors

You can modify the anchor servers.

### About this task

To modify anchors, follow these steps:

## Procedure

1. In the navigation pane, click **Discovery Anchors**. The Discovery Anchors page is displayed.
2. Edit the anchor by clicking the **Edit** icon . beside the anchor. The Discovery Anchor page is displayed with the current settings for the anchor.
  - a. In the Select Scope Set Restriction pane, specify whether to use the anchor server across all defined discovery scopes or limit the anchor server to a scope that you specify.

**Note:** The anchor server scope should be restricted to the systems in that network section.

- b. If you chose to limit the anchor server to a specified scope, select the scope set for this anchor server.
- c. Click **Save**. The anchor is displayed in the Discovery Anchors page.

## Deleting anchors

You can delete anchor servers that you no longer need.

### About this task

**Note:** You cannot delete the root server anchor.

To delete an anchor, follow these steps:

### Procedure

1. In the navigation pane, click **Discovery Anchors**. The Discovery Anchors page is displayed.
2. Click the **Delete** icon . beside the anchor that you want to delete.
3. Click **OK** to confirm that you want to delete the anchor.

---

## Discovery gateways

A discovery gateway is a proxy server that has access to Microsoft Windows systems in your environment. Before Technical Support Appliance version 1, release 3, it was necessary to specify a discovery gateway before the Technical Support Appliance could discover information about systems running MicrosoftWindows. With version 1, release 3, the Technical Support Appliance can discover this information without a discovery gateway. However, any gateway servers that are defined for prior versions of the Technical Support Appliance will continue to function.

## Displaying discovery gateways

You can display the defined discovery gateway servers.

### About this task

To display the existing discovery gateway servers, click **Discovery Gateways** in the navigation pane. The Discovery Gateways page is displayed.

## Modifying discovery gateways

With version 1, release 3, the Technical Support Appliance can discover information about systems that are running Microsoft Windows without a

discovery gateway server. However, any discovery gateways that are defined for prior releases of the Technical Support Appliance continue to function. You can modify these existing discovery gateways.

### About this task

To modify gateways, follow these steps:

#### Procedure

1. In the navigation pane, click **Discovery Gateways**. The Discovery Gateways page is displayed.
2. To edit a gateway, click the **Edit** icon beside the gateway. The Discovery Gateway page is displayed with the current settings for the gateway server.
  - a. In the Select Scope Set Restriction pane, specify whether to use the gateway server across all defined discovery scopes or limit the gateway server to a scope that you specify.
  - b. If you chose to limit the gateway server to a specified scope, select the scope set for this gateway server.
  - c. Click **Save**. The gateway is displayed in the Discovery Gateways page.

## Deleting gateways

You can delete discovery gateway servers that you no longer need.

### About this task

To delete a gateway, follow these steps:

#### Procedure

1. In the navigation pane, click **Discovery Gateways**. The Discovery Gateways page is displayed.
2. Click the **Delete** icon beside the discovery gateway that you want to delete.
3. Click **OK** to confirm that you want to delete the discovery gateway.

---

## Discovery schedule

Discoveries are scheduled to ensure that discovered data is always current and accurate. You can view the discovery schedule and details of the last discoveries, modify the discovery schedule, and disable scheduled discoveries. You can also run a discovery whenever you choose and save the discovered data to a location that you specify.

## Viewing the discovery schedule

You can display the summary information about a discovery schedule.

### About this task

To view the discovery schedule, follow these steps:

#### Procedure

In the navigation pane, click **Discovery Schedule**. The Discovery Schedule page is displayed.

The Schedule pane displays the next scheduled run and the scheduled run times. The History pane displays the status and more details of the currently running and previous discovery jobs.

## Modifying the discovery schedule

The Technical Support Appliance provides a default schedule for the discovery process to run at specified times. You can modify this schedule according to your needs.

### About this task

To modify the discovery schedule, follow these steps:

### Procedure

1. In the navigation pane, click **Discovery Schedule**. The Discovery Schedule page is displayed.  
The Schedule pane displays the next scheduled run and the scheduled run times. The History pane displays the status and more details of the currently running and previous discovery jobs.
2. Click **Edit Schedule**. The Discovery Schedule page is displayed.
  - a. In the Enable Schedule pane, select whether you want to enable or disable scheduled discoveries.
  - b. Use the **At hour** and **At minute** drop-down lists to select a new time.
  - c. For the **On days** field, select the appropriate check box to select different or more days of the week.
3. Click **Save**. The Discovery Schedule page is displayed again, with the new schedule shown.

### Related concepts:

“Discovery schedule” on page 3

Discoveries run on scheduled days and times to ensure that discovered data is always current and accurate. The Technical Support Appliance has a default discovery schedule that you can modify for your needs. You can also view details, history, and the state of the last discovery that was run.

## Disabling the discovery schedule

You can disable scheduled discoveries.

### Procedure

To disable scheduled discoveries, follow these steps:

1. In the navigation pane, click **Discovery Schedule**. The Discovery Schedule page is displayed.
2. Click **Edit Schedule**. The Discovery Schedule page is displayed.
3. In the Enable Schedule pane, select **Do not perform scheduled discovery**.
4. Click **Save**. The Discovery Schedule page is displayed and the Schedule pane shows that the scheduled discovery is disabled. You can enable scheduled discoveries by clicking **Perform scheduled discovery**.

## Running the discovery

You can run a discovery on demand, rather than wait for the next scheduled discovery. You can run a discovery on all defined discovery scopes or on specific discovery scopes.

### Procedure

To run a discovery on all defined scopes, follow these steps:

1. In the navigation pane, click **Discovery Schedule**. The Discovery Schedule page is displayed.
2. Click **Run Discovery Now**. The History section is updated indicating that the discovery is running.

**Note:** When you are running a discovery that requires anchors, ensure that each anchor is included in the discovery scope. For example, to discover a target that is in a scope set assigned to an anchor, both the anchor and the scope set must be included in the discovery run. For information, see “Setting up discovery Scopes” on page 20.

### Running the discovery on specific scope sets

You can run a discovery on a specific scope set.

#### Procedure

To run a discovery on a specific scope set, follow these steps:

1. In the navigation pane, click **Discovery Scopes**. The Discovery Scopes page is displayed. This page displays a list of all scope sets that are defined for this Technical Support Appliance.
2. To run a discovery on a specific scope set, click the **Run** icon  for that scope set.

### Running discovery on specific scopes

You can run a discovery on a specific scope.

#### Procedure

To run a discovery on a specific scope, follow these steps:

1. In the navigation pane, click **Discovery Scopes**. The Discovery Scopes page is displayed.
2. Click the scope set that contains the scope on which you want to run a discovery. The Discovery Scope Set page is displayed. This page displays all the scopes that are defined for that scope set.
3. To run a discovery on a specific scope, click the **Run** icon  for that scope.

## Saving the discovered data collection

You can save the last discovered data collection.

### About this task

To save the last discovered data collection, follow these steps:

## Procedure

1. In the navigation pane, click **Transmission Schedule**. The Transmission Schedule page is displayed.
2. Click **Download Last Collection**. Specify where you want to save the data.

**Note:** Depending on the amount of data, the save operation might take some time.

---

## Discovery history

You can view the details of a discovery after it completes and download a diagnostics log file for the discovery.

### Procedure

To view the discovery history or download a diagnostics log file, follow these steps:

1. In the navigation pane, click **Discovery History**. The Discovery History page is displayed. A list of discovery entries is displayed. Each entry displays the status, name, and the start and end times for a discovery.
2. To display more information about an entry in the History Entries list, click the name of the history entry.

The Entry information pane displays information about the selected discovery. The Discovery scopes pane displays the scopes that were used for the selected discovery.

3. To download a diagnostics log file for a discovery, click the **Download** icon for the discovery.

---

## Transmission schedule

Transmission of data is scheduled to ensure that discovered data is regularly sent to IBM Support. You can view the transmission schedule and the details of the last transmissions, modify the transmission schedule, and disable scheduled transmissions. You can also send the data to IBM whenever you choose.

### Viewing the transmission schedule

You can view the summary information about a transmission schedule.

#### About this task

To view the transmission schedule, follow these steps:

### Procedure

In the navigation pane, click **Transmission Schedule**. The Transmission Schedule page is displayed.

The Schedule pane displays the next scheduled run and the scheduled run times. The History pane displays the status and additional details of the currently running and previous transmission jobs.

## Modifying the transmission schedule

The Technical Support Appliance provides a default schedule for the transmission process to run at specified times. You can modify this schedule according to your needs.

### About this task

To modify the transmission schedule, follow these steps.

### Procedure

1. In the navigation pane, click **Transmission Schedule**. The Transmission Schedule page is displayed.  
The Schedule pane displays the next scheduled run and the scheduled run times. The History pane displays the status and additional details of the currently running and previous transmission jobs.
2. Click **Edit Schedule**. The Transmission Schedule page is displayed.
  - a. Use the **At hour** and **At minute** drop-down lists to select a new time.
  - b. For the **On days** field, select the appropriate check box to select different or additional days of the week.
3. Click **Save**. The Transmission Schedule page is displayed again, with the new schedule shown.

### Related concepts:

“Transmission schedule” on page 3

Discovered data is securely packaged and transmitted to IBM Support on regularly scheduled days and times to ensure that IBM has the most current and accurate information. A default transmission schedule, that you can modify for your needs, is provided. You can also run transmissions on demand.

## Disabling the transmission schedule

You can disable scheduled data transmissions.

### Procedure

To disable scheduled transmissions, follow these steps:

1. In the navigation pane, click **Transmission Schedule**. The Transmission Schedule page is displayed.
2. Click **Edit Schedule**. The Transmission Schedule page is displayed.
3. In the Enable Schedule pane, select **Do not perform scheduled transmission**.
4. Click **Save**. The Discovery Schedule page is displayed and the Schedule pane shows that the scheduled discovery is disabled. You can enable scheduled transmissions by clicking **Perform scheduled transmission**.

## Running the transmission

You can run a transmission on demand, rather than wait for the next scheduled transmission.

### About this task

To run the transmission immediately, follow these steps:

## Procedure

1. In the navigation pane, click **Transmission Schedule**. The Transmission Schedule page is displayed.
2. Click **Run Transmission Now**. The History section is updated indicating that the transmission is running.

**Tip:** To save the results of the data collection, click **Download Last Collection** and specify a location for the results.

Depending on the amount of data, the save operation might take some time.

---

## Status information

The Technical Support Appliance provides summary information, logs, and reports to enable you to quickly find information about jobs, discovered inventory, and product information.

You can display the high level summary information about jobs, inventory, and product information by clicking **Summary** in the navigation pane. The Summary page refreshes frequently to show the most up-to-date summary information. The Summary page includes the following information:

- **System Status**  
The System Status pane displays the status of current services and tasks being performed. You can display the pages for the services displayed by clicking the name of the service in the System Status pane.
- **Job Summary**  
The Job Summary pane displays a summary of current jobs.
- **Inventory Summary**  
The Inventory Summary pane displays a list of discovered inventory. You can click on this pane to display the inventory report.
- **Product Information**  
The Product Information pane displays product information, such as the host name, version, and ID of the Technical Support Appliance along with the versions of custom sensors and command-line interfaces that the Technical Support Appliance uses for the custom sensors that interact with storage devices.

## Viewing the activity log

The activity log displays log messages for the discovery and transmission processes. You can click the entries in the activity log to view more information.

You can display the activity log by clicking **Activity Log** in the navigation pane. A list of log entries is displayed. Each entry displays the message, the severity, and the time the activity occurred.

**Note:** Because discoveries are run on individual scope sets, there might be multiple log entries for a full discovery.

To display extended details about any activity log entry, click the message for that entry.

To save the log files to your computer, click **Download All Logs**.

**Note:** This selection downloads all logs, even those logs that are used only when the Technical Support Appliance is reporting problems to IBM.

To clear the log, click **Clear Log**.

## Viewing the inventory report

The inventory report displays information about discovered inventory.

You can display the inventory report by clicking **Inventory Report** in the navigation pane.

To refresh this display, click **Run Report Now**.

---

## Passwords

You use passwords to secure the Technical Support Appliance user accounts.

### Changing your password

Change the Technical Support Appliance user password.

#### About this task

To change the password, follow these steps.

#### Procedure

1. In the navigation pane, click **Administration > Password**. The Password page is displayed.
2. Enter your current password in the **Current password** field.
3. Enter the new password in the **New password** field.  
The password must adhere to the following rules:
  - Must be at least 8 characters long
  - Must contain at least one alphabetic and one non-alphabetic character
  - Must not contain the user name
  - Must not be the same as any of the previous eight passwords
  - Must be changed at least once every 90 days, but must not be changed more than once each day
4. Enter the new password again in the **Confirm password** field. The two passwords that you enter are compared to confirm that they match before the password is saved.
5. Click **Save**.

#### What to do next

**Important:** Ensure that you record the new password for future reference. It is not possible to recover a password, so if the password is lost or forgotten, you cannot sign in to the Technical Support Appliance. If you lose or forget your password, contact IBM Support.

---

## Security

You can access and modify security functions and utilities for the Technical Support Appliance.

The Security page lists the available security utilities. On this page, you can configure SSH key pair authentication, generate or upload and install a server certificate, or modify session timeout settings.

## Configuring key pair authentication

You must configure discovery credentials on the Technical Support Appliance to enable discovery on target computer systems. You can configure credentials that use user name and password authentication or OpenSSH Version 2 key-pair authentication. The advantage of using key-pair authentication is that you do not have to maintain passwords in the Technical Support Appliance for service accounts that exist on the target computer systems.

### Before you begin

Before you configure discovery credentials that use key-pair authentication, ensure the following:

- OpenSSH is installed on the target computer systems
- The SSH daemon is running on the target computer systems
- The service account is created on the target computer systems and has the necessary authorizations for the relevant platform
- No firewalls are blocking access from the Technical Support Appliance to the target computer systems on port 22

For more information about SSH, see the following sources:

#### OpenSSH

<http://www.openssh.org/manual.html>

#### SSH.com

<http://www.ssh.com/index.php/support-overview/product-documentation.html>

### About this task

Configuring discovery credentials that use key-pair authentication requires that you perform the following tasks:

- Generate the key pair
- Download the generated public key
- Deploy the public key to the target computer systems that you want to discover
- Create the discovery credential

### Procedure

#### Generate the key pair

1. In the navigation pane, click **Administration > Security**. The Security page is displayed.
2. Enter a passphrase in the **Passphrase** field.

**Important:** The passphrase must be at least eight characters long and contain at least one numeric and one alphabetic character. A good passphrase is 10 - 30 characters long and consists of both numeric characters and random upper and lowercase alphabetic characters.

3. Enter the passphrase again in the **Confirm Passphrase** field. The two passphrases that you enter are compared to confirm that they match before the passphrase is saved.
4. Save the passphrase in a secure location for use in later configuration steps.
5. Click **Generate SSH Server Public/Private Key Pair**. A message that the key pair has been generated along with a **Download SSH Server Public Key** button is displayed in the SSH Server Key Status pane.

#### **Download the generated public key**

6. Click **Download SSH Server Public Key** to download the public key on the system that you are using to sign on to the Technical Support Appliance. This is the key that you deploy on the target computer systems.

#### **Deploy the public key to the target systems**

7. Use any available process or utility to deploy the public key to the target computer systems.

**Note:** Utilities exist in most SSH implementations to assist with deploying public keys. For example, OpenSSH includes an `ssh-copy-id` utility that you can use to deploy the public key to the target computer systems.

If the `ssh-copy-id` utility is available on the system that you are using to sign on to the Technical Support Appliance, you can deploy the public key to a target system by running the following command:

```
ssh-copy-id -i id_rsa.pub serviceaccount@remotehost
```

If the `ssh-copy-id` utility is not available, insert the contents of the public key file (`id_rsa.pub`) into the `$HOME/.ssh/authorized_keys` file for the service account on each target computer system where you want to use key-pair authentication.

#### **Create the discovery credential**

8. In the navigation pane, click **Discovery Credentials**. The Discovery Credentials page is displayed.
9. Click **Add New Credentials**. The New Discovery Credentials page is displayed.
  - a. In the **Name** field, type an identifying name for the credential.
  - b. In the Credential Type drop-down list, select **Computer System**.
  - c. In the Enter Access Information pane, specify the following information:

##### **User name**

The user name for the service account on the target computer system.

##### **Password**

The passphrase you specified when generating the public/private key pair.

##### **Confirm password**

Enter the passphrase again. The two passphrases that you enter are compared to confirm that they match before the passphrase is saved.

##### **Authentication type**

Select **Public Key Infrastructure (PKI)**.

- d. Click **Save**. The new credential is displayed in the Discovery Credentials page.

The Technical Support Appliance can now run discoveries against the target computer systems that have this service account configured and the public key installed, and login to the operating system using OpenSSH Version 2 key-based authentication.

## Installing an SSL server certificate

The Technical Support Appliance uses a default SSL server certificate to secure data transmission. For added security, you can install a self-signed SSL server certificate that is unique to this Technical Support Appliance, or upload your own SSL server certificate.

### Before you begin

If you want to upload a custom certificate, you must acquire the certificate. You will need to provide the location of the certificate file, and the password for the certificate.

### About this task

**Note:** When you install a certificate, the Technical Support Appliance is automatically restarted.

To install an SSL server certificate, follow these steps:

### Procedure

1. In the navigation pane, click **Administration > Security**. The Security page is displayed.
2. If you want to install a self-signed server certificate, click **Generate and install a new Self-signed Certificate**. This certificate is unique to this Technical Support Appliance.
3. If you want to install a custom server certificate, follow these steps.
  - a. Enter the password for the certificate in the **Certificate password** field.
  - b. Enter the password again in the **Confirm password** field. The two passwords that you enter are compared to confirm that they match before the password is saved.
  - c. Specify the location of the custom certificate file in the **Custom certificate file** field.
  - d. Click **Upload and install a Custom Certificate**.

### Results

If the server certificate installation completes successfully, the next time you log in to the Technical Support Appliance, you will see the certificate along with a message prompting you to specify whether to trust the certificate.

## Modifying session timeout settings

For security, the user is logged out of the Technical Support Appliance after a period of inactivity. You can prevent the Technical Support Appliance from automatically logging out the user, or change the amount of time before the user is logged out.

## Disabling session timeout

You can prevent the Technical Support Appliance from automatically logging the user out after a period of inactivity by disabling session timeout.

### About this task

To disable session timeout, follow these steps:

#### Procedure

1. Clear the **Disable Session Timeout** check box.
2. Click **Change Session Timeout Settings**.

## Modifying the session timeout value

By default the user is logged out after 1,200 seconds or 20 minutes of inactivity. You can increase the amount of time before the user is logged out by modifying the session timeout value.

### About this task

To modify the session timeout value, follow these steps:

#### Procedure

1. In the **Session timeout** field, enter the time in seconds before the Technical Support Appliance logs out the user.

**Note:** This session timeout value cannot be less than 1,200 seconds.

2. Click **Change Session Timeout Settings**.

---

## Backup and restore

You can back up and restore the Technical Support Appliance configuration.

### Configuration summary

Use this option to view a summary of the current Technical Support Appliance configuration before you save it.

To display the Technical Support Appliance configuration summary, follow these steps:

1. In the navigation pane, click **Administration > Backup and Restore**. The Backup and Restore page is displayed.
2. Click **View Summary**.

### Backup

Use this option to save a copy of the Technical Support Appliance configuration.

To back up the Technical Support Appliance configuration, follow these steps:

1. In the navigation pane, click **Administration > Backup and Restore**. The Backup and Restore page is displayed.
2. Enter a password to protect the configuration file.
3. Enter the password again in the **Confirm password** field. The two passwords that you enter are compared to confirm that they match before the password is saved.

4. Click **Backup**.
5. You can optionally specify a name and location for the backup configuration file.

**Note:** The backup operation is intended for migrating the Technical Support Appliance configuration. Restoring a backup configuration file after changing the Technical Support Appliance configuration can result in unexpected consequences.

6. Click **Save** to save the configuration file on the system that you are using to sign on to the Technical Support Appliance.

## Restore

Use this option to restore a previously saved copy of the configuration.

**Important:** Restoring the configuration in certain situations can result in unexpected consequences. Contact IBM Support before restoring a Technical Support Appliance configuration.

To restore a Technical Support Appliance configuration, follow these steps:

1. In the navigation pane, click **Administration > Backup and Restore**. The Backup and Restore page is displayed.
2. Click **Browse** to locate and select the configuration file that you want to restore.
3. Enter the password that is used to protect the configuration file.

**Note:** A password is required only if one was specified when the configuration file was backed up.

4. Click **Restore**.

The restore job is displayed in the Job Summary pane of the Summary page. When the restoration is complete, you are prompted to restart the system.

---

## Update

You can check for and download updates for the Technical Support Appliance.

### About this task

To check for updates for the Technical Support Appliance, follow these steps:

### Procedure

1. In the navigation pane, click **Administration > Update**. The Check for Update page is displayed.
2. Click **Check for Update**. The Update Availability page lists any available updates.
3. To install the updates, click **Perform Update Now**. Upon completion of the update, the Technical Support Appliance is automatically restarted.

---

## Logging and trace

You can view and modify the Technical Support Appliance diagnostic trace settings. Modifying these settings can affect performance so do this only if directed by IBM Support.

To view and modify the Technical Support Appliance diagnostic trace settings, follow these steps:

1. In the navigation pane, click **Administration > Logging and Trace**. The Trace Level page is displayed indicating the current trace setting (Error, Warning, Information, Debug, or Trace).
2. If needed, you can change the trace setting by clicking the radio button beside the trace setting that you want.
3. Click **Save**.

The Summary page is displayed.

---

## Shutdown

You can suspend or resume Technical Support Appliance operations, or shut down and then restart or power off the Technical Support Appliance.

Shutdown takes several minutes to complete.

### Suspend Operations

This action temporarily stops the Technical Support Appliance. All discovery and transmission operations are stopped, and no information is reported to IBM until operations are resumed.

To suspend the Technical Support Appliance operations, follow these steps:

1. In the navigation pane, click **Administration > Shutdown**. The Shutdown page is displayed.
2. Click **Suspend**.

### Resume Operations

This action resumes the temporarily stopped Technical Support Appliance. All discovery and transmission operations are resumed, and information is reported to IBM as scheduled.

To resume the Technical Support Appliance operations, follow these steps:

1. In the navigation pane, click **Administration > Shutdown**. The Shutdown page is displayed.
2. Click **Resume**.

### Shutdown and Restart

This action shuts down and then restarts the Technical Support Appliance. All existing network connections are temporarily lost. You must open a new browser and login again.

To shut down and restart the Technical Support Appliance, follow these steps:

1. In the navigation pane, click **Administration > Shutdown**. The Shutdown page is displayed.
2. Click **Restart**.

## Shutdown and Power Off

This action shuts down and powers off the Technical Support Appliance. All discovery and transmission operations cease and your infrastructure is not reported until the Technical Support Appliance is restarted.

To shut down and power off the Technical Support Appliance, follow these steps:

1. In the navigation pane, click **Administration** > **Shutdown**. The Shutdown page is displayed.
2. Click **Shutdown**.

---

## Tools

The Technical Support Appliance provides tools to help you when setting up the Technical Support Appliance or environment.

You can access these tools by clicking **Tools** in the navigation pane.

### Network Tools

Use the Network tools page to obtain diagnostic tools and information for the network protocols that the Technical Support Appliance uses.

To access these diagnostic tools, click **Tools** > **Network Tools** in the navigation pane. The Network Tools page is displayed.

The Network Tools page is divided into tabbed pages. Click any tab to display the page that corresponds to that tab.

**Ping** Use this page to send an echo request to a remote host to check if the host is accessible and to receive information about the host name or IP address.

#### **Traceroute**

Use this page to display the path that packets take to a remote host.

#### **Test SSH**

Use this page to test whether a remote host is accessible with SSH using the discovery credentials defined for the host.

#### **Interfaces**

Use this page to display the statistics for the network interfaces that are currently configured.

#### **Ethernet**

Use this page to display settings for the Ethernet cards that are currently configured.

#### **Address**

Use this page to display IP addresses for the network interfaces that are currently configured.

#### **Routes**

Use this page to display the Kernel IP routing tables and corresponding network interfaces.

**ARP** Use this page to display the contents of the Address Resolution Protocol (ARP) connections.

#### **Sockets**

Use this page to display information about the TCP/IP sockets.

**IPs** Use this page to display information about the IP packet filter rules.

## Unknown Devices

You can display information about devices that the Technical Support Appliance has discovered, but is not able to fully identify.

To display these unknown devices, click **Tools > Unknown Devices** in the navigation pane. The Unknown Devices page is displayed.

You can click any entry in the Unknown IPs list to display additional information about that device.

## Advanced Storage

The Technical Support Appliance automatically detects most types of storage devices. You can define discovery credentials for these storage devices on the Discovery Credentials page. If you want to discover SAN Volume Controller (SVC) or V7000 storage devices, you must manually create definitions for these storage devices. You can view, add, modify, and delete SVC and V7000 storage device definitions on the Advanced Storage page.

### Displaying SVC or V7000 storage devices

You can display SVC or V7000 storage devices that can be discovered by the Technical Support Appliance.

#### About this task

You can display the SVC or V7000 storage devices by clicking **Tools > Advanced Storage** in the navigation pane. The Advanced Storage page is displayed. The SVC or V7000 storage devices that the Technical Support Appliance can discover are displayed in the Devices table.

### Adding SVC or V7000 storage device definitions

You can define SAN Volume Controller (SVC) or V7000 storage devices for the Technical Support Appliance to discover.

#### About this task

To define a storage device, follow these steps:

#### Procedure

1. In the navigation pane, click **Tools > Advanced Storage**. The Advanced Storage page is displayed.
2. Click **Add New Device**. The Storage Device page is displayed.
3. In the Describe Address or Host pane, enter the IP address or host name for the storage device.
4. In the Enter Access Information pane, specify the user name and SSH key file for the storage device.
5. Click **Save**. The new SVC or V7000 storage device is displayed on the Advanced Storage page.

### Modifying SVC or V7000 storage device definitions

You can modify definitions for SVC or V7000 storage devices.

## About this task

To modify a SVC or V7000 storage device definition, follow these steps:

### Procedure

1. In the navigation pane, click **Tools > Advanced Storage**. The Advanced Storage page is displayed.
2. Edit the storage device definition by clicking the Edit icon  next to the storage device. The Storage Device page is displayed.
3. In the Describe Address or Host pane, you can change the IP address or host name for this device.
4. In the Enter Access Information pane, you can change the access information for this device.
5. Click **Save**. The changed storage device definition is displayed in the Advanced Storage page.

## Deleting SVC or V7000 storage device definitions

You can delete SVC or V7000 storage device definitions.

## About this task

To delete a SVC or V7000 storage device definition, follow these steps:

### Procedure

1. In the navigation pane, click **Tools > Advanced Storage**. The Advanced Storage page is displayed.
2. Click the Delete icon  beside the storage device definition that you want to delete.
3. Click **OK** to confirm that you want to delete the storage device definition.

---

## Accessibility

The Technical Support Appliance does not interfere with the accessibility features for supported browsers. For a comprehensive list of accessibility features please visit the accessibility support page for the supported browser that you are using. For a list of supported browsers, see “Required internet browsers” on page 5.

The publications for this product are in Adobe Portable Document Format (PDF) and should be compliant with accessibility standards. If you experience difficulties using the PDF files and want to request a web-based format for a publication, email a request to the following address:

[icfeedback@us.ibm.com](mailto:icfeedback@us.ibm.com)

Or, you can mail a request to the following address:

International Business Machines Corporation  
Information Development  
3605 Hwy 52 North  
Rochester, MN, U.S.A 55901

In the request, be sure to include the publication title, “IBM Technical Support Appliance Setup Guide” in the subject line of your note.

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.



---

## Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785  
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan Ltd.  
1623-14, Shimotsuruma, Yamato-shi  
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

---

## Trademarks

IBM, the IBM logo, and [ibm.com](http://ibm.com) are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.



