ARX® Secure Agent Installation Guide

810-0013-00

Publication Date

This manual was published on August 30, 2012.

Legal Notices

Any modifications to this device, unless expressly approved by the manufacturer, can void the user's authority to operate this equipment under part 15 of the FCC rules.

Canadian Regulatory Compliance

This Class A digital apparatus complies with Canadian ICES-003.

Standards Compliance

This product conforms to the IEC, European Union, ANSI/UL and Canadian CSA standards applicable to Information Technology products at the time of manufacture.

Acknowledgments

This product includes software from several third-party vendors. Each vendor is listed below with the applicable copyright.

Revision History

June 2004 - Rev A

July 2004 - Rev B

September 2004 - Rev C

October 2004 - Rev D - Software version 1.2

December 2004 - Rev E - updated License notice

March 2005 - Rev F - Software version 1.2.10

October 2005 - Rev G - Software version 2.1

April 2006 - Rev H - Software version 2.3 (platform-name change)

June 2006 - Rev J, updates for Software Release 2.4

October 2006 - Rev K, new links for multiple CLI users guides

October 2006 - Rev L, Software version 2.4.2

December 2007 - Rev M, change CLI examples

March 2008 - Rev N, update with F5 format

October 2008 - Rev P, re-brand the OS

June 2009 - Rev Q, clarifications for Windows-domain entries

November 2009 - Rev R, add “pre-win2k-name” option to the configuration; add upgrade instructions

March 2010 - Rev S, add pop-ups concerning AV setup and optional reboot

April 2010 - Rev T, remove upgrade procedure; must uninstall before new install
October 2010 - Rev U, updates for Software Release 5.02.000
June 2011 - Rev V, updates for Software Release 6.00.000
September 2011 - Rev W, trademark updates for Software Release 6.01.000
July 2012 - Rev W, minor updates for Software Release 6.02.000
October 2012 - Rev X, minor updates for Software Release 6.03.000

Table of Contents

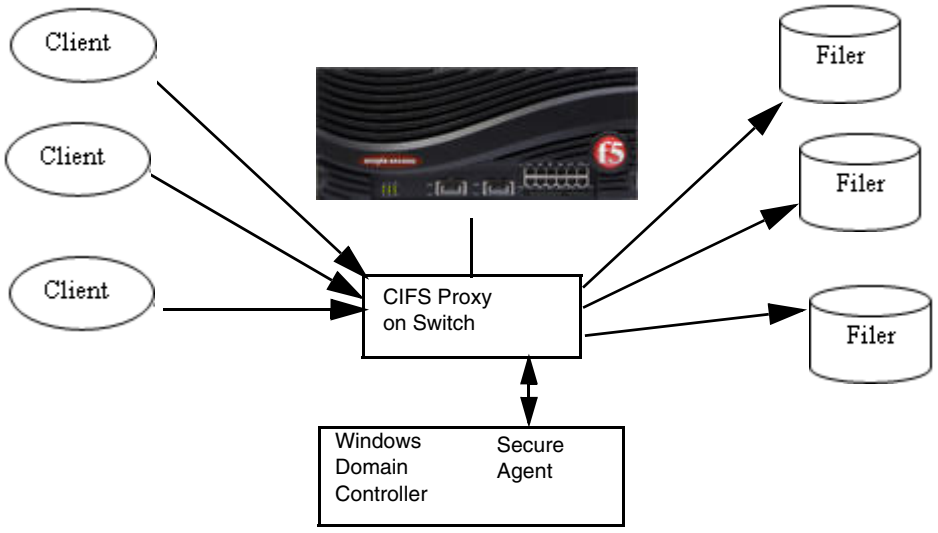
1

Introduction

- Overview
- Software Components and Requirements
- Audience for this Manual
- Document Conventions
- Related Documents
- Contacting Customer Service

Overview

This manual describes how to install and manage the ARX® Secure Agent™ software. This software provides NT LAN Manager (NTLM) and NTLMv2 authentication service on behalf of the ARX. The Secure Agent software is installed on a Microsoft Windows domain controller where security objects, such as usernames and passwords, are configured and maintained in a database. The Windows domain controller assists the CIFS proxy on the switch in verifying responses from front-end clients and responding to requests for back-end filer access. The following diagram shows a sample topology.



Software Components and Requirements

The Secure Agent software contains the following Windows-based runtime components:

- **ARX Secure Agent** — The Secure-agent software runs as a Windows Service, displayed as the "Acopia Secure Agent." A setup wizard installs and starts the service. The service is configured with a startup type of "automatic," so that Windows restarts the Secure Agent on reboot.
- **ARX Secure Agent Management applet** — The management user interface used to monitor statistics and view/modify Secure Agent settings. See Chapter 4, Managing Secure Agent for details.

Windows Support

Windows Domain Controllers (DCs)

ARX Secure Agent is supported on Windows Domain Controllers (DCs) running Microsoft Windows 2000, Windows 2003, or Windows 2008. Secure Agent assists the switch in authenticating client connections, maintaining a client's identity to back-end filers, and processing access control lists.

Secure Agent software is installed on the DCs associated with the back-end filers. For example, if Filer A is in Windows domain, DOMAINA, you install Secure Agent software on the DOMAINA domain controller. On the switch, you then configure an instance of Secure Agent for the Windows domain by specifying the IP address, password, and port (optional) where the Secure Agent software is installed.

The Windows DC requires a network connection on the server subnet or through a static route that uses a gateway on the server subnet.

See Chapter 3 for information about configuring Secure Agent on the switch.

Multiple Domains and Trust Relationships

The ARX also supports Microsoft networks in multiple domains that share two-way trust relationships. You configure the "trust relationship" on the switch by defining multiple instances of Secure Agent (called *NTLM-auth-servers*) and assigning them to ARX namespaces. You install the Secure Agent software on each domain controller in the trust; the ARX uses these DCs to authenticate clients in each domain. For example, if a Windows network contains DOMAINA, DOMAINB, and DOMAINC, and they all share a two-way trust with each other, you install the Secure Agent software on each domain controller. On the switch, you configure a Secure Agent instance (NTLM-auth server) for each domain *(*DOMAINA,

DOMAINB, and DOMAINC), then assign it to the relevant namespace. See Chapter 3, Configuring the ARX for information about configuring Secure Agent on the switch.

Access Privilege

Secure Agent software installation/configuration requires Windows users with *Administrator* privilege.

Anti-Virus Application Settings

The Secure Agent software accesses the Domain Controller's (DC's) database, so anti-virus (AV) applications may prevent the Secure Agent software from functioning. Before you install the Secure Agent on a DC, consult AskF5 Solution SOL10026, which describes all necessary AV settings. That solution is posted on http://askf5.f5.com.

Password Security

The connection between the ARX and the Secure Agent is an authenticated TCP connection. Authentication is accomplished through a password shared by the switch and the Secure Agent software. All data sent on the connection is encrypted using a generated session key. Each TCP connection uses a different session key. *Actual password or password hashes are never passed through the connection*. No more information is passed over this connection than what is available in the clear in a normal CIFS session between two Windows computers.

Installation Overview

To install and configure ARX Secure Agent software:

1. Install the Secure Agent software on each domain controller, as required in your network. See Chapter 2, Installing Secure Agent, for instructions.
2. On the ARX, configure a Secure Agent instance (NTLM-auth-server) for each Secure Agent installation/domain controller. See Chapter 3, Configuring the ARX, for instructions.
3. Assign a Secure Agent instance to the relevant ARX namespace. See Chapter 3 for instructions.
4. Set up a CIFS service through the ARX CLI. See the *ARX® CLI Storage-Management Guide* for configuration information.

Audience for this Manual

This manual is intended for network administrators responsible for connecting the switch to front-end and back-end network and storage resources at the enterprise data center.

Document Conventions

This manual uses the following conventions, when applicable:

- `courier` text represents system output
- **bold** text represents user input
- *italic* text appears for variable input, emphasis, and book titles

◆ Note

Notes provide additional or helpful information about the subject text.

Related Documents

In addition to this guide, the following ARX documentation is also available:

- *ARX®-VE Installation Guide*
- *ARX®–500 Hardware Installation Guide*
- *ARX®–2000 Hardware Installation Guide*
- *ARX®–4000 Hardware Installation Guide*
- *ARX® CLI Network-Management Guide*
- *ARX® CLI Storage-Management Guide*
- *ARX CLI Maintenance Guide*
- *ARX® CLI Reference*
- Release Notes

Contacting Customer Service

You can use the following methods to contact F5 Networks Customer Service:

F5 Networks Online Knowledge Base Online repository of answers to frequently-asked questions.	http://support.f5.com
F5 Networks Services Support Online Online customer support request system	https://websupport.f5.com
Telephone	Follow this link for a list of Support numbers: http://www.f5.com/support/support-services/contact/

2

Installing Secure Agent

This chapter describes how to install the Secure Agent software using the installation setup wizard. It contains the following sections:

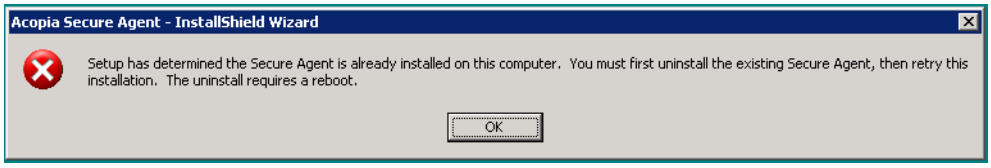
- Installing the Software on a DC
- Viewing Log Information

Installing the Software on a DC

If you have a former version of the Secure Agent running on this DC, you must uninstall it before you install this version. The Secure Agent uninstall process, described later in the chapter, requires a reboot.

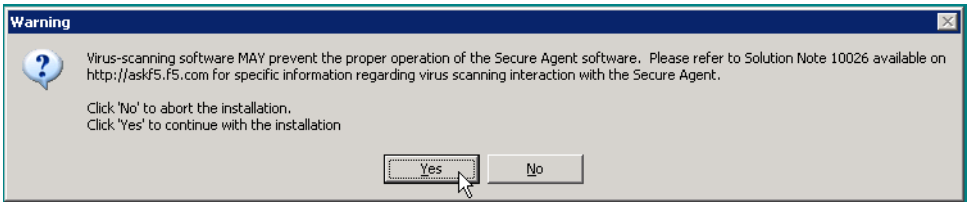
To install a new Secure Agent application on your DC, follow these steps:

1. Download the proper Secure Agent software from https://downloads.f5.com/esd/productlines.jsp. Choose the 32-bit or the 64-bit software package, depending on your DC hardware.
2. Unzip the software package and double-click on the setup.exe file.
   a) If an instance of Secure Agent is already installed on this DC, the following pop-up informs you that you must uninstall it first:



   Instructions for uninstalling appear below. After the uninstall, restart this procedure.

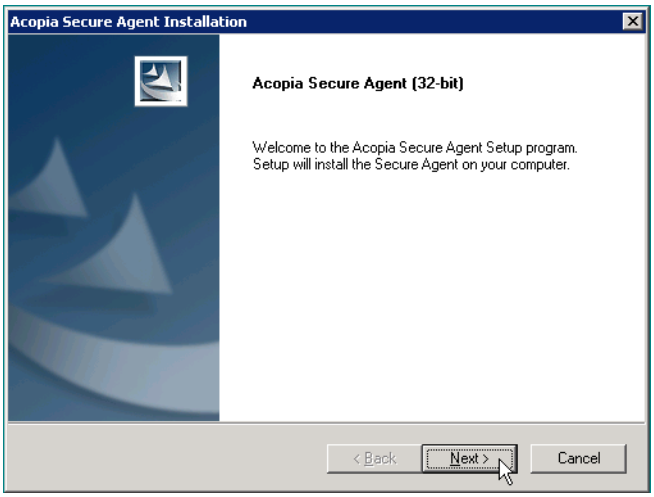
   b) If no instance of Secure Agent is currently installed, the following warning pops up:



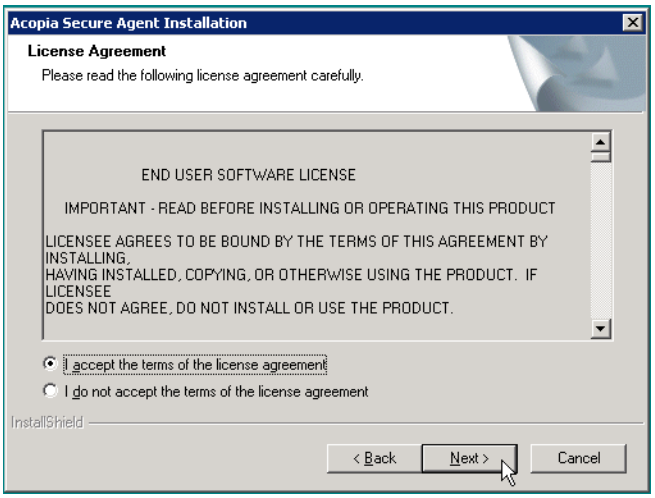
   Follow the instructions in the pop-up, which refer you to AskF5 Solution SOL10026 on http://askf5.f5.com/.

3. After you allow the Secure Agent to run on the DC, click **Yes** to continue.

   This invokes the following screen:

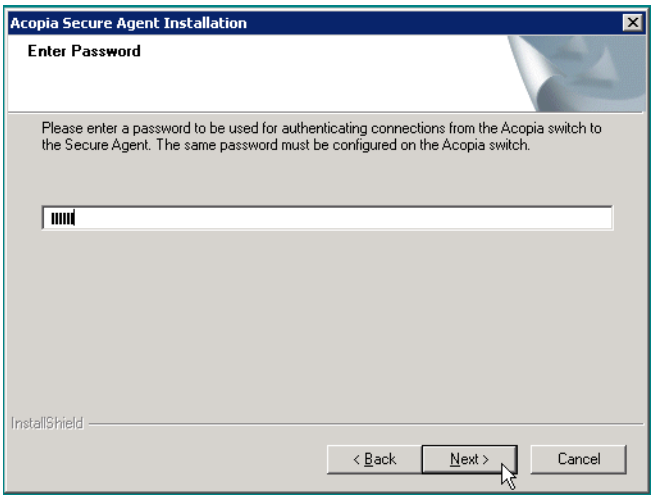


4. Click **Next** to proceed.
5. The wizard displays the License Agreement screen.



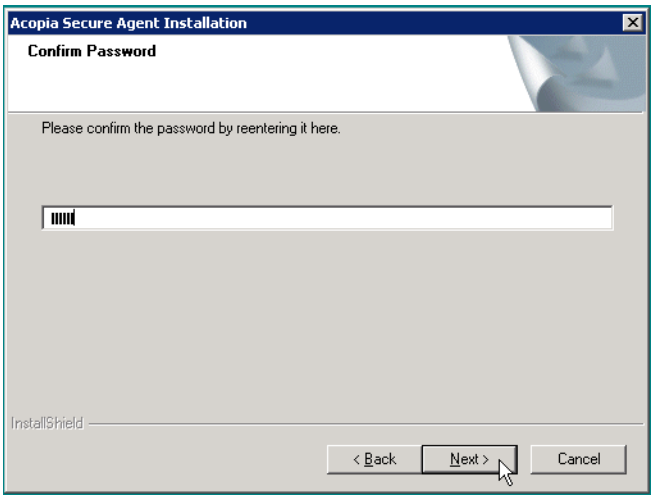
6. Click the radio button to accept the terms of the F5 license agreement, then click **Next**.

7. Enter a password from 4-64 characters that the ARX will use to authenticate TCP connections. Then click **Next**.

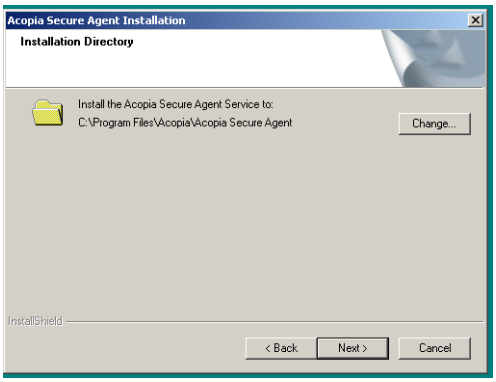


This same password must also be defined on the ARX, as described in Chapter 3, Configuring the ARX. For more information about Secure Agent and authentication, see Password Security, on page 1-5.

8. Re-enter the password to confirm.

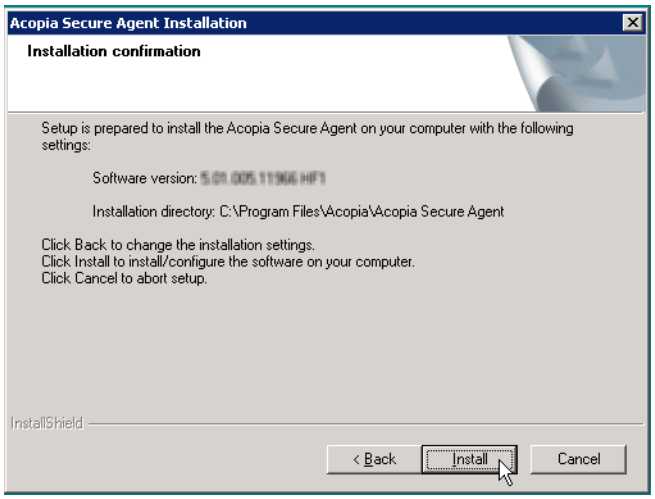


9. Specify where to install the software; accept the default or click **Change** to specify a different path.

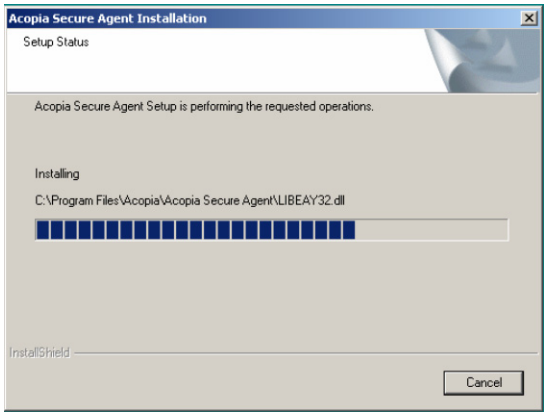


10. Click **Next**.

11. Review the setup wizard settings, then click **Install** to proceed with the installation.

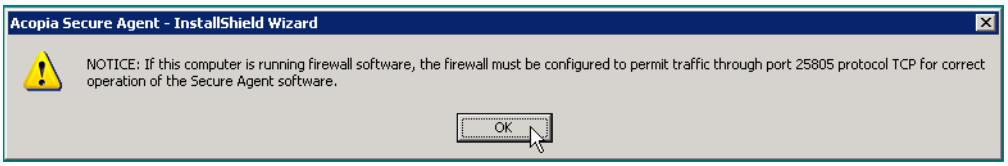


The wizard displays the installation status screen.

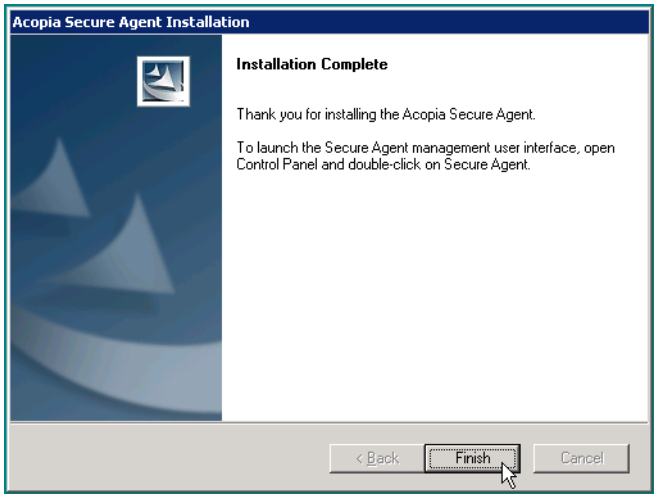


12. A pop-up warns you that the local firewall must allow TCP traffic over the Secure Agent port. You can change the Secure Agent port in its applet interface, described below.

    Click **OK** to continue:



13. When installation is complete, the wizard displays the last screen.



14. Click **Finish** to exit the wizard.

Confirm that your firewall leaves open the TCP port required for Secure Agent access.

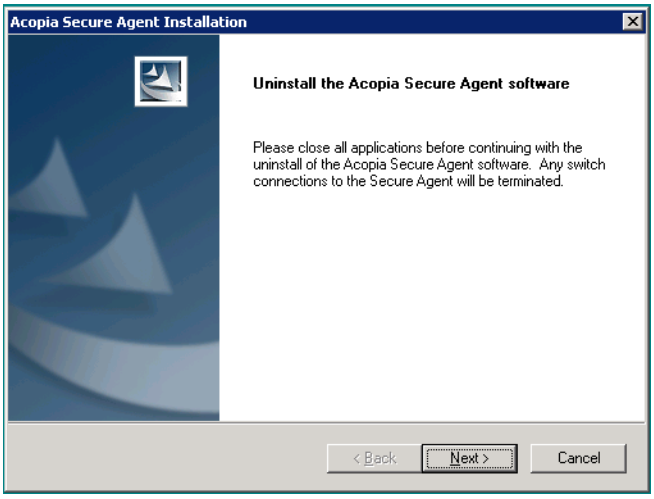
Uninstalling the Secure Agent

You must uninstall the Secure Agent before you install a new version.

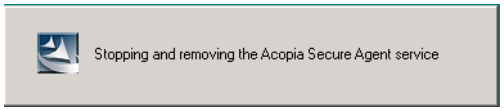
Important

The uninstall causes the DC to reboot.

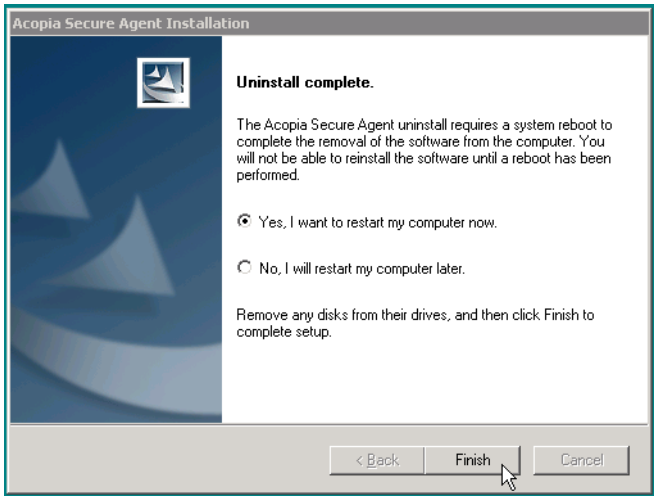
1. Use the standard Add/Remove Programs interface on your DC. This invokes the following pop-up. Close all other applications, then click **Next** to continue:



2. The following appears while the uninstall process removes the Secure Agent software:



Then a pop-up announces the completion of the uninstall process:



The pop-up informs you that a reboot is required to complete installation, and offers and option to reboot now.

3. Choose one of the reboot options and click **Finish**.

Viewing Log Information

Following Secure Agent software installation, you can view log information in %TEMP%\acopia-secure-agent-install.log (usually located in C:\Documents and Settings\Administrator\Local Settings\Temp).

3

Configuring the ARX

This chapter describes how to modify the ARX configuration to enable NTLM/NTLMv2 authentication through Secure Agent software installed on a Windows Domain Controller (DC). It contains the following sections:

- Before You Begin
- Modifying Switch Software

Before You Begin

Verify that all switch installation, network, namespace, and global server (CIFS) configuration tasks are complete.

Modifying Switch Software

Following Secure Agent software installation and before setting up a CIFS file service on the switch, you must modify the switch configuration to enable NTLM/NTLMv2 authentication through Secure Agent. Follow these steps to configure an NTLM authentication server for each instance of Secure Agent installed on a DC host system.

To configure the ARX to use NTLM Secure Agent:

1. From gbl mode in the CLI, enter the following:

```
ntlm-auth-server name
windows-domain domain [pre-win2k-name former-domain]
password
Password: password
Validate Password: password
port port-number
ip address ip-address
exit
```

name (1-128 characters) is an arbitrary name you choose for this Secure Agent (authentication server) instance. Typically, the name matches the hostname or domain name where this instance of Secure Agent is running.

domain (1-64 characters) is the name of the Windows domain where this instance of Secure Agent is installed. Use the fully-qualified-domain name (FQDN), such as “boston.ma.gov.” Clients that authenticate with shorter variations (such as “boston”) will also connect to this Secure Agent.

pre-win2k-domain *former-domain* (optional, 1-15 bytes) is useful if this domain has a pre-Windows-2000 alias with no relation to the FQDN, such as “CAPITOL.” Specify the former domain name here. If you enter any lower-case letters, the CLI converts them to upper-case as needed.

password (4-64 characters) is the password used to authenticate connections between the switch and Secure Agent.

port-number (optional; the default is 25805) is the TCP port over which Secure Agent transactions will occur.

ip-address is the IP address of the DC host system running this instance of Secure Agent. The address must be on the server subnet or reachable through a static route.

◆ Note

If the DC is not on the server subnet, the static route to it must go through a router on the server subnet. This applies even if the DC is in a client subnet. To add a static route to the DC, see Adding a Static Route, on page 4-10 of the ARX® CLI Network-Management Guide.

For example, the following configuration supports two domains, "MEDARCH.ORG" and a legacy domain name, "NTNET."

```
bstnA(gbl)# ntlm-auth-server dc1
This will create a new NTLM Server.

Create NTLM Server 'dc1'? [yes/no] yes
bstnA(gbl-ntlm-auth-srv[dc1])# windows-domain MEDARCH.ORG pre-win2k-name NTNET
bstnA(gbl-ntlm-auth-srv[dc1])# ip address 192.168.25.109
bstnA(gbl-ntlm-auth-srv[dc1])# password
Password: mypa$$w0rd
Validate Password: mypa$$w0rd
bstnA(gbl-ntlm-auth-srv[dc1])# exit
bstnA(gbl)# ...
```

2. Assign the Secure Agent authentication server to a namespace. All CIFS services that export from the namespace use the namespace's Secure Agent server.

   From gbl mode in the CLI, the following command enters gbl-ns mode:

   namespace *namespace-name*

   namespace-name is the namespace name.

   Then, from gbl-ns mode, assign this Secure Agent to the namespace with the following command:

   ntlm-auth-server *name*

   name is the name of a Secure Agent authentication server (ntlm-auth-server) instance to associate with this namespace. You can assign one NTLM authentication server to multiple namespaces.

   For example, this command sequence assigns the above server, "dc1," to the "medarcv" namespace:

```
bstnA(gbl)# namespace medarcv

This will create a new namespace.

Create namespace 'medarcv'? [yes/no] yes
bstnA(gbl-ns[medarcv])# ntlm-auth-server dc1
bstnA(gbl-ns[medarcv])# ...
```

3. Use the following command(s) to configure NTLM and/or NTLMv2 authentication for the namespace. You invoke these from gbl-ns mode, too:

   cifs authentication ntlm

   and/or

   cifs authentication ntlmv2

   For example, this command sequence configures both NTLM and NTLMv2 for the "medarcv" namespace:

```
bstnA(gbl)# namespace medarcv

This will create a new namespace.

Create namespace 'medarcv'? [yes/no] yes
bstnA(gbl-ns[medarcv])# cifs authentication ntlm
bstnA(gbl-ns[medarcv])# cifs authentication ntlmv2

% INFO: To use NTLMv2 with the Acopia Secure Agent, all agent instances must support
NTLMv2 (requires agent version 5.1.0 or later).

bstnA(gbl-ns[medarcv])# ...
```

Undoing Switch Settings

To remove any of these settings, use the no forms of the commands. For example,

no ntlm-auth-server myserver

removes the Secure Agent authentication server named "myserver."

Where there is a default, the no command reverts the setting to the default. For example,

no port

changes the port number back to 28505.

Listing all Configured NTLM-Authentication Servers

From any CLI mode, use the show ntlm-auth-server command to list all configured Secure Agent authentication servers, along with their configuration parameters:

show ntlm-auth-server

For example:

```
bstnA(gbl)# show ntlm-auth-server

Name                                Server           Version    Capabilities  Status
Domain Name                                          Pre-Win2k Domain
-------------------------------------------------------------------------------
dc1                                 192.168.25.109   V5.01.000  NTLM, NTLMv2  Reachable
MEDARCH.ORG                                          NTNET

dc2                                 192.168.25.102   V5.00.000  NTLM          Reachable
```

```
MEDARCH.ORG                                          NTNET

bstnA(gbl)# ...
```

Showing Statistics for One NTLM-Authentication Server

From any CLI mode, use the name of a server with the show ntlm-auth-server command to see its statistics:

show ntlm-auth-server *name*

where *name* (1-128 characters) is the name of the desired Secure Agent authentication server.

The output ends with a table of ARX namespaces that use the Secure Agent server.

For example:

```
bstnA(gbl)# show ntlm-auth-server dc1

******************** SECURE AGENT STATISTICS ******************
Agent IP   : 192.168.25.109
Agent Port : 25805

Uptime: 0 days, 7 hours, 58 minutes and 37 seconds
Current Connections: 9
Failed connection attempts: 2674
Successful connection attempts: 2727
Account Scan Interval: 300
Software version: Version 5.01.000.11899 (Sep 24 2009 20:55:35) [jc] [x86]
Capabilities: NTLM, NTLMv2, Session Key
bstnA(gbl)# ...
```

Sample Configuration

The following command sequence configures an NTLM authentication server named “dc1” (as above), shows it, and uses it in the “medarcv” namespace:

```
bstnA(gbl)# ntlm-auth-server dc1
This will create a new NTLM Server.

Create NTLM Server 'dc1'? [yes/no] yes
bstnA(gbl-ntlm-auth-srv[dc1])# windows-domain MEDARCH.ORG pre-win2k-name NTNET
bstnA(gbl-ntlm-auth-srv[dc1])# ip address 192.168.25.109
bstnA(gbl-ntlm-auth-srv[dc1])# password
Password: mypa$$w0rd
Validate Password: mypa$$w0rd
bstnA(gbl-ntlm-auth-srv[dc1])# exit
bstnA(gbl)# show ntlm-auth-server

Name                              Server           Version    Capabilities  Status
Domain Name                                        Pre-Win2k Domain
-------------------------------------------------------------------------------
dc1                               192.168.25.109   V5.01.000  NTLM, NTLMv2  Reachable
MEDARCH.ORG                                        NTNET

bstnA(gbl)# namespace medarcv
```

```
bstnA(gbl-ns[medarcv])# ntlm-auth-server dc1
bstnA(gbl-ns[medarcv])# ...
```

4

Managing Secure Agent

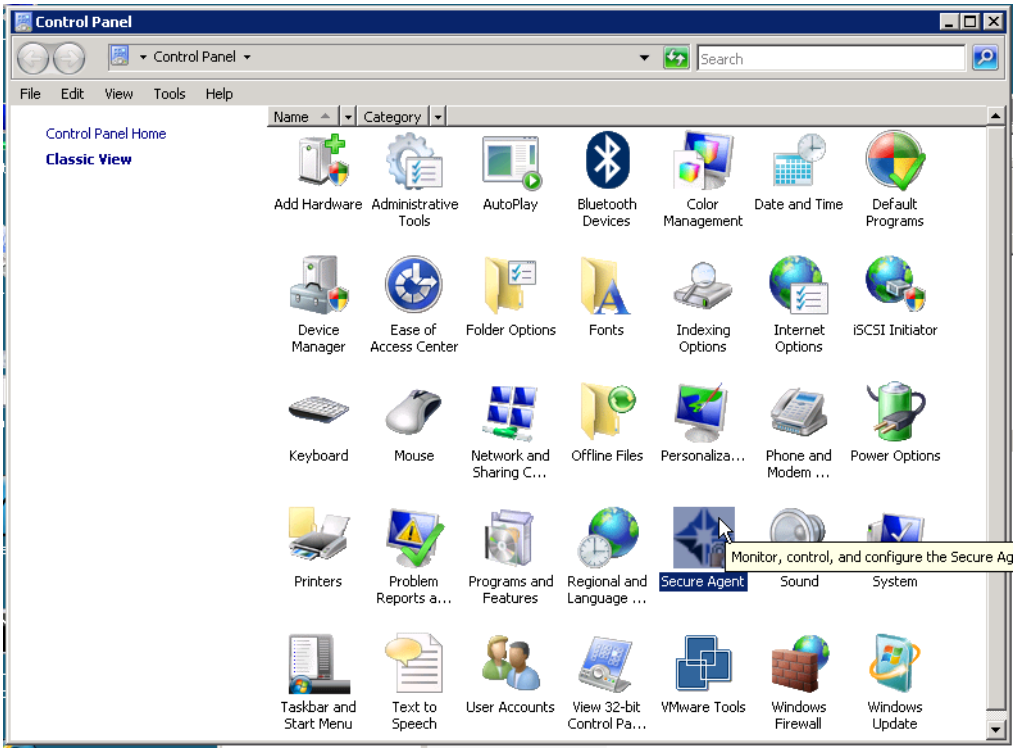
This chapter describes how to use the Secure Agent Management applet, which enables you to monitor real-time statistics and view and modify settings, such as the password and TCP port connection to the switch.

- Invoking the Secure-Agent Management Applet
- Resetting Statistics
- Changing the Password or TCP Port
- Stopping and Restarting the Secure Agent Service

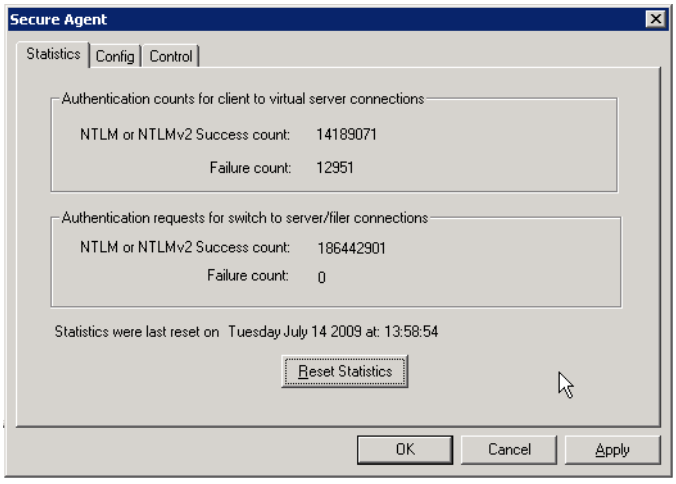
Invoking the Secure-Agent Management Applet

To start the management applet:

1. Select **Start->Settings->Control Panel** (on the Windows domain controller).
2. Double-click the **Secure Agent** icon to start the applet.

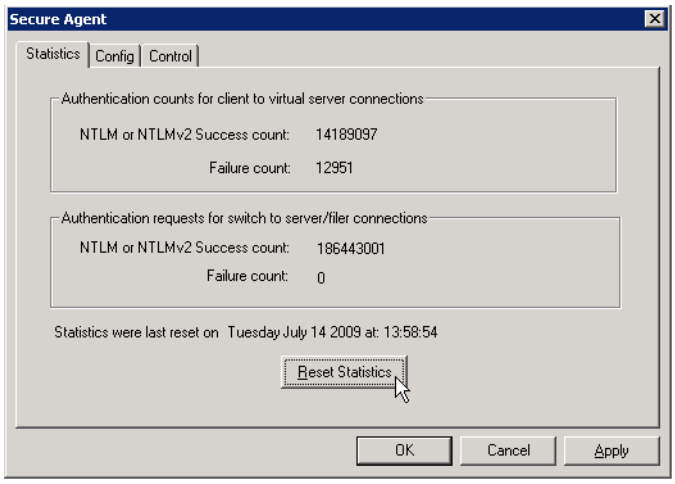


The system displays the Statistics tab screen. This screen shows real-time statistics information for authentication requests coming from clients to the switch and from the switch to back-end filers.



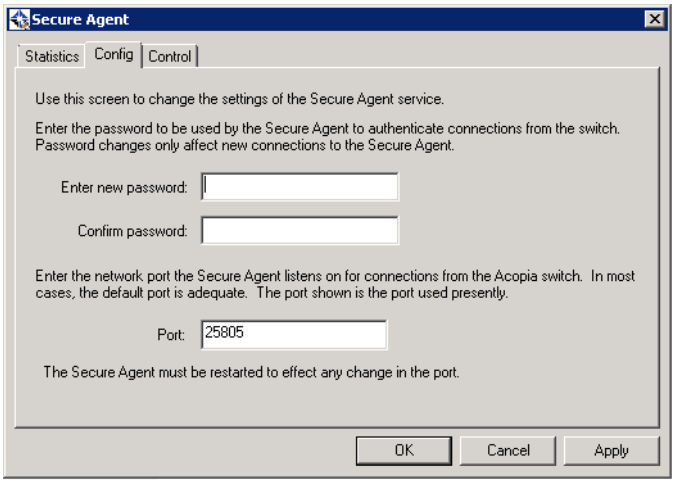
Resetting Statistics

To reset the counters, click **Reset Statistics**. As Secure Agent processes authentication requests, the management applet automatically updates the counters.



Changing the Password or TCP Port

Click the **Config** tab to change the password. You can also change the TCP port used to listen for incoming requests from the ARX. Confirm that the local firewall application allows communication over this port.

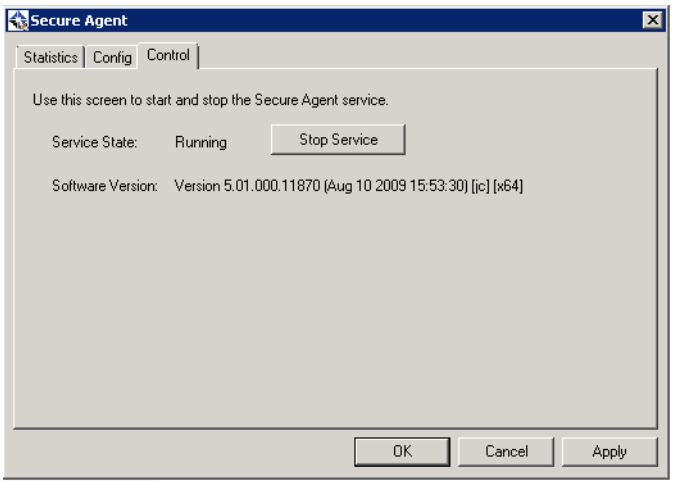


◆ Note

If you change the password, new connections to Secure Agent must use the new password. Current connections are not affected.

Stopping and Restarting the Secure Agent Service

To view the current version and operational state, click the **Control** tab.



1. Click the **Stop Service** button to stop or start Secure Agent service, as applicable.

Important

The ARX cannot perform NTLM or NTLMv2 authentications while the Secure Agent is stopped.

Index