TREND MICRO™

Apex Central™

Patch 3

Installation and Upgrade Guide

Centralized Security Management for Endpoints

Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

http://docs.trendmicro.com/en-us/enterprise/apex-central.aspx

Trend Micro, the Trend Micro t-ball logo, Trend Micro Apex Central, Trend Micro Apex One, Control Manager, and OfficeScan are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Document Part No.: APEM39503/220311

Release Date: March 2022

Protected by U.S. Patent No.: 5,623,600; 5,889,943; 5,951,698; 6,119,165

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Evaluate this documentation on the following site:

http://www.trendmicro.com/download/documentation/rating.asp

Table of Contents

Preface

Preface v

Documentation vi

Audience vii

Document Conventions vii

Terminology viii

Chapter 1: Introducing Apex Central

About Apex Central 1-2

Key Features and Benefits 1-2

Apex Central Architecture 1-4

Chapter 2: Installation Planning

Identifying Deployment Architecture and Strategy 2-2
- Understanding Single-Site Deployment 2-3
- Understanding Multiple-Site Deployment 2-4
- Planning for Network Traffic 2-8

Apex Central Setup Flow 2-9

Testing Apex Central at One Location 2-9
- Preparing for the Test Deployment 2-10
- Selecting a Test Site 2-11
- Beginning the Test Deployment 2-11
- Evaluating the Test Deployment 2-11

Server Distribution Plan 2-11
- Understanding Administration Models 2-12
- Understanding Apex Central Server Distribution 2-13
- Single-Server Topology 2-13
- Multiple-Server Topology 2-13

Network Traffic Plan 2-13
Understanding Apex Central Network Traffic 2-14

Source of Network Traffic 2-15
Log Traffic 2-15
Trend Micro Management Communication Protocol Policies 2-17
Product Registration Traffic 2-17
Policy Deployment 2-18

Deploying Updates 2-18

Data Storage Plan 2-19
Database Recommendations 2-20
ODBC Driver 2-21
Authentication 2-21

Web Server Plan 2-21

Chapter 3: Installation

System Requirements 3-2

Installing the Apex Central Server 3-8
Apex Central Installation Flow 3-9
Installing All Required Components 3-10
Specifying the Installation Location 3-13
Activating the Product and Services 3-14
Specifying Apex Central Web Server Settings 3-15
Specifying Backup Settings 3-17
Setting Up the Root Account 3-19
Configuring Database Information 3-20

Chapter 4: Post-installation Tasks

Automatic Post-installation Tasks 4-2

Verifying the Server Installation or Upgrade 4-2

Activating Your Software 4-4
Activating Apex Central 4-4
Converting to the Full Version 4-5

Configuring Active Directory Connection Settings 4-5

Configuring User Accounts 4-8

Downloading the Latest Components 4-8

Configuring Event Notifications 4-9

Chapter 5: Upgrades and Migration

Upgrading to Apex Central 5-2
- Supported Versions for Upgrade 5-2
- Server Files to Back Up Before Migration 5-3
- Pre-migration Checklist 5-3

Upgrade and Migration Scenarios 5-5
- Upgrade Flow 5-5
- Scenario 1: Upgrading a Control Manager Server to Apex Central 5-5
- Scenario 2: Migrating to a Fresh Apex Central Installation Using the Agent Migration Tool 5-7

Planning Apex Central Agent Migration 5-8
- Rapid Upgrade 5-8
- Phased Upgrade 5-8

Migrating the Apex Central Database 5-9
- Migrating a Apex Central SQL Database to Another SQL Server 5-9

Chapter 6: Post-Migration Tasks

Verifying a Successful Upgrade or Migration 6-2

Migrating Apex One Server Settings to Apex Central 6-3

Enabling Application Control 6-4

Enabling Vulnerability Protection 6-6

Enabling Endpoint Sensor 6-7

Configuring Apex One Server Settings for Endpoint Sensor ... 6-9

Chapter 7: Uninstallation

Removing Apex Central 7-2

Manually Removing Apex Central 7-3
Removing the Apex Central Application 7-3

Chapter 8: Apex Central System Checklists

Server Address Checklist 8-2
Port Checklist 8-3
Apex Central Conventions 8-4
Core Processes and Configuration Files 8-4
Communication and Listening Ports 8-6

Index

Index IN-1

Preface

Preface

Welcome to the Trend Micro Apex Central™ *Installation and Upgrade Guide*. This document discusses requirements and procedures for installing the Apex Central server, and upgrading from a previous installation.

Topics in this section:

Documentation

Apex Central documentation includes the following:

Document	Description
Readme file	Contains a list of known issues and may also contain late-breaking product information not found in the Online Help or printed documentation
Installation and Upgrade Guide	A PDF document that discusses requirements and procedures for installing the Apex Central **Note** The Installation and Upgrade Guide may not be available for minor release versions, service packs, or patches.
System Requirements	A PDF document that discusses requirements and procedures for installing Apex Central
Administrator's Guide	A PDF document that provides detailed instructions of how to configure and manage Apex Central and managed products, and explanations on Apex Central concepts and features
Online Help	HTML files compiled in WebHelp format that provide "how to's", usage advice, and field-specific information. The Help is also accessible from the Apex Central console
Widget and Policy Management Guide	A PDF document that explains how to configure dashboard widgets and policy management settings in Apex Central
Automation Center	Online user guides and references that explain how to use the Apex Central Automation APIs: https://automation.trendmicro.com/apex-central/home
Data Protection Lists (Chapter 1 only)	A PDF document that lists predefined data identifiers and templates for Data Loss Prevention
Knowledge Base	An online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following website: http://success.trendmicro.com

Download the latest version of the PDF documents and readme at:

http://docs.trendmicro.com/en-us/enterprise/apex-central.aspx

Audience

Apex Central documentation is intended for the following users:

- Apex Central Administrators: Responsible for Apex Central installation, configuration, and management. These users are expected to have advanced networking and server management knowledge.
- Managed Product Administrators: Users who manage Trend Micro products that integrate with Apex Central. These users are expected to have advanced networking and server management knowledge.

Document Conventions

The documentation uses the following conventions.

TABLE 1. Document Conventions

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
Italics	References to other documents
`Monospace`	Sample command lines, program code, web URLs, file names, and program output
Navigation > **Path**	The navigation path to reach a particular screen For example, **File** > **Save** means, click **File** and then click **Save** on the interface

Convention	Description
Note	Configuration notes
Tip	Recommendations or suggestions
Important	Information regarding required or default configuration settings and product limitations
WARNING!	Critical actions and configuration options

Terminology

The following table provides the official terminology used throughout the Apex Central documentation:

Terminology	Description
Administrator (or Apex Central administrator)	The person managing the Apex Central server
Security Agent	The managed product program installed on an endpoint
Components	Responsible for scanning, detecting, and taking actions against security risks
Apex Central console, web console, or management console	The web-based user interface for accessing, configuring, and managing a Apex Central **Note** Consoles for integrated managed products are indicated by the managed product name. For example, the Apex One web console.

Terminology	Description
Managed endpoint	The endpoint where the managed product Security Agent is installed
Managed product	A Trend Micro product that integrates with Apex Central
Managed server	The endpoint where the managed product is installed
Server	The endpoint where the Apex Central server is installed
Security risk	The collective term for virus/malware, spyware/grayware, and web threats
Product service	Apex Central services hosted through Microsoft Management Console (MMC).
Dual-stack	Entities that have both IPv4 and IPv6 addresses
Pure IPv4	An entity that only has an IPv4 address
Pure IPv6	An entity that only has an IPv6 address

Chapter 1

Introducing Apex Central

This section introduces Trend Micro Apex Central™ and provides an overview of its features and capabilities.

Topics include:

- *About Apex Central on page 1-2*
- *Key Features and Benefits on page 1-2*
- *Apex Central Architecture on page 1-4*

About Apex Central

Trend Micro Apex Central™ is a web-based console that provides centralized management for Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels. Administrators can use the policy management feature to configure and deploy product settings to managed products and endpoints. The Apex Central web-based management console provides a single monitoring point for antivirus and content security products and services throughout the network.

Apex Central enables system administrators to monitor and report on activities such as infections, security violations, or virus/malware entry points. System administrators can download and deploy components, such as antivirus pattern files, scan engines, and antispam rules, throughout the network to ensure up-to-date protection. Apex Central allows both manual and pre-scheduled updates, and allows the configuration and administration of products as groups or as individuals for added flexibility.

Key Features and Benefits

Apex Central provides the following features and benefits.

Feature	Benefits
Active Directory integration	Apex Central supports integration with multiple Active Directory forests and allows you to import Active Directory groups in addition to users. You can also enable Active Directory Federation Services (ADFS) authentication to allow users or groups from federated business partners across an extranet to securely log on to your Apex Central network.
Dashboard	Use the **Dashboard** tabs and widgets for extensive visibility of managed product and Apex Central information about threat detections, component statuses, policy violations, and more.

Feature	Benefits
Security Posture	Use the **Security Posture** tab to gain instant insights into the antivirus pattern and Data Loss Prevention compliance status, critical threat detections, as well as resolved and unresolved events on your network.
User/Endpoint Directory	View detailed information about all the users and endpoints within the Apex Central network and any security threat detections.
Product Directory	System administrators can immediately deploy configuration modifications to managed products or even run a manual scan from the Apex Central web console during a virus/malware outbreak.
Global Policy Management	System administrators can use policies to configure and deploy product settings to managed products and endpoints from a single management console to ensure consistent enforcement of your organization's virus/malware and content security policies.
Logs	Use a single management console to view consolidated logs from all registered managed products without having to log on to each individual product console.
Event Notifications	Keep administrators informed of network events at all times by configuring Apex Central to send notifications by email, Windows syslog, SNMP trap, or an in-house or industry-standard application used by your organization.
Reports	Create comprehensive reports from custom or static templates to obtain the actionable information you need to ensure network protection and security compliance.
Component Updates	Securely download and deploy antivirus patterns, antispam rules, scan engines, and other antivirus or content security components to help ensure that all managed products are up to date.
Connected Threat Defense	Apex Central brings together a host of Trend Micro products and solutions to help you detect, analyze, and respond to targeted attacks and advanced threats before they unleash lasting damage.
Secure communication infrastructure	Apex Central uses a communications infrastructure built on the Secure Socket Layer (SSL) protocol and can even encrypt messages with authentication.

Feature	Benefits
Role-based Administration	Grant and control access to the Apex Central web console by assigning specific web console privileges to administrators and providing only the tools and permissions necessary to perform specific tasks.
Command Tracking	Command Tracking allows you to continuously monitor whether commands executed using the Apex Central web console, such as antivirus pattern updates and component deployment, have successfully completed.
License management	Deploy new Activation Codes or reactivate existing Activation Codes on managed products.
Security Agent installation	Download Security Agent installation packages for Apex One or Apex One (Mac) directly from the Apex Central console.
Two-Factor Authentication	Two-Factor Authentication provides extra security on user accounts by requiring users to type the verification code generated by the Google Authenticator app in order to sign in to Apex Central.
Browser support	This version of Apex Central includes support for the following: • Microsoft™ Internet Explorer™ • Microsoft™ Edge™ • Google™ Chrome™

Apex Central Architecture

Trend Micro Apex Central™ provides a means to control Trend Micro products and services from a central location. This application simplifies the administration of a corporate virus/malware and content security policy.

The following table describes the components that Apex Central uses.

Component	Description
Apex Central server	Acts as a repository for all data collected from the agents. The Apex Central server includes the following features: • An SQL database that stores managed product configurations and logs Apex Central uses the Microsoft SQL Server database (`db_ApexCentral.mdf`) to store data included in logs, managed product information, user account, network environment, and notification settings. • A web server that hosts the Apex Central web console • A mail client that delivers event notifications through email messages Apex Central can send notifications to individuals or groups of recipients about events that occur on the Apex Central network. Send event notifications by email, SNMP trap, syslog, or any in-house/industry standard application used by your organization to send notifications. • A report server that generates antivirus and content security product reports The Apex Central report is an online collection of figures about security threat and content security events that occur on the Apex Central network.
Trend Micro Management Communication Protocol	MCP handles the Apex Central server interaction with managed products that support the next generation agent. MCP agents install with managed products and use one/two way communication to communicate with Apex Central. MCP agents poll Apex Central for instructions and updates.
Web Service Integration communication	An agent-less integration model that allows Apex Central to communicate with managed products

Component	Description
Web-based management console	Allows an administrator to manage Apex Central from virtually any computer with an Internet connection and web browser The Apex Central management console is a web-based console published on the Internet through the Microsoft Internet Information Server (IIS) and hosted by the Apex Central server. It lets you administer the Apex Central network from any computer using a compatible web browser.
Widget Framework	Allows an administrator to create a customized dashboard to monitor the Apex Central network.

Chapter 2

Installation Planning

This chapter helps you plan for deployment and manage a Apex Central test deployment.

Topics include:

- *Identifying Deployment Architecture and Strategy on page 2-2*
- *Apex Central Setup Flow on page 2-9*
- *Testing Apex Central at One Location on page 2-9*
- *Server Distribution Plan on page 2-11*
- *Network Traffic Plan on page 2-13*
- *Source of Network Traffic on page 2-15*
- *Deploying Updates on page 2-18*
- *Data Storage Plan on page 2-19*
- *Web Server Plan on page 2-21*

Identifying Deployment Architecture and Strategy

Deployment is the process of strategically distributing Apex Central servers in your network environment to facilitate and provide optimal management of antivirus and content security products.

Deploying enterprise-wide, client-server software like Apex Central to a network requires careful planning and assessment.

For ease of planning, Trend Micro recommends two deployment architectures:

- **Single-site deployment**: Refers to distributing and managing servers, managed products, and endpoints from a single Apex Central located in a central office. If your organization has several offices but has fast and reliable local and wide area network connections between sites, single-site deployment still applies to your environment.
- **Multiple-site deployment**: Refers to distributing and managing Apex Central servers in an organization that has main offices in different geographical locations.

Understanding Single-Site Deployment

Single-site deployment refers to distributing and managing servers, managed products, and endpoints from a single Apex Central located in a central office.

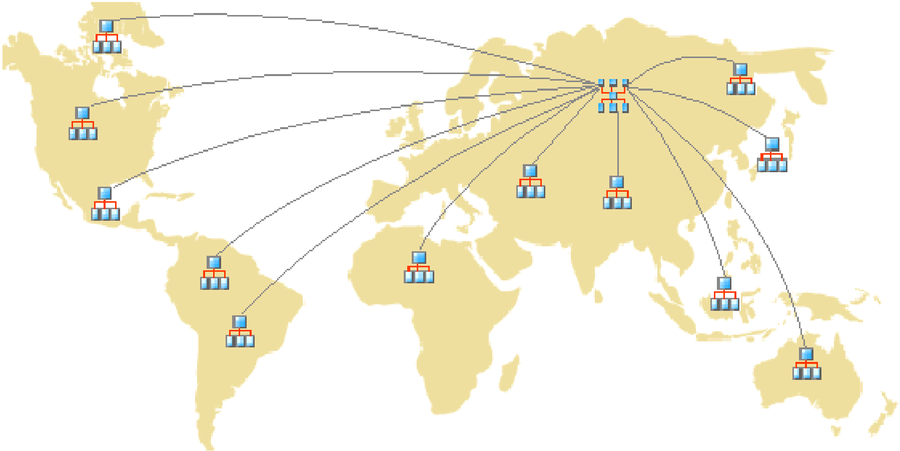


FIGURE 2-1. A single-site deployment using a single Apex Central server

Before deploying Apex Central to a single site, complete the following tasks:

1. Determine the number of managed products and endpoints
2. Plan for the optimal ratios of server, managed products and endpoints
3. Designate the Apex Central server

Determining the Number of Managed Products and Endpoints

Determine how many managed products and endpoints structures you plan to manage with Apex Central. You will need this information to decide what kind and how many Apex Central servers you need to deploy, as well as where to put these servers on your network to optimize communication and management.

Planning for the Optimal Ratios of Server to Managed Products

The most critical factor in determining how many managed products and endpoints a single Apex Central server can manage on a local network is the agent-server communication.

Use the recommended system requirements as a guide in determining the CPU and RAM requirements for your Apex Central network.

Designating Apex Central Servers

Based on the number of managed products and endpoints, decide and designate your Apex Central server.

Locate your Windows servers, and then select the ones to assign as Apex Central servers. You also need to determine if you need to install a dedicated server.

When selecting a server that will host Apex Central, consider the following:

- The CPU load
- Other functions the server performs

If you are installing Apex Central on a server that has other uses (for example, application server), Trend Micro recommends that you install on a server that is not running mission-critical or resource-intensive applications.

Depending on your network topology, you may need to perform additional site-specific tasks.

Understanding Multiple-Site Deployment

As with single-site deployment, collect relevant network information and identify how this information relates to deploying Apex Central to your multiple sites.

Given the uniqueness of each network, exercise judgment as to how many Apex Central servers would be optimal.

Deploy Apex Central servers in a number of different locations, including the demilitarized zone (DMZ) or the private network. Position the Apex Central server in the DMZ on the public network to administer managed products, endpoints, or other servers and access the Apex Central web console over the Internet.

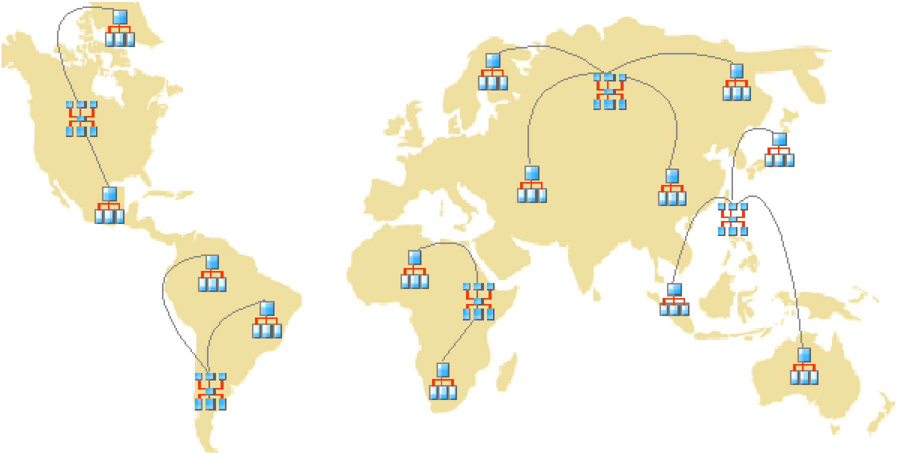


FIGURE 2-2. A multi-site deployment using multiple Apex Central servers

Consider the following for multi-site deployment:

- Group managed products, endpoints, or servers
- Determine the number of sites
- Determine the number of managed products, endpoints, and servers
- Plan for network traffic
- Decide where to install the Apex Central server

Grouping Managed Products

Consider the following when you group managed products:

TABLE 2-1. Considerations Grouping Managed Products

CONSIDERATION	DESCRIPTION
Company network and security policies	If different access and sharing rights apply to the company network, group managed products, endpoints, and servers according to company network and security policies.
Organization and function	Group managed products, endpoints, and servers according to the company's organizational and functional division. For example, have two Apex Central servers that manage the production and testing groups.
Geographical location	Use geographical location as a grouping criterion if the location of the managed products, endpoints, and servers affects the communication between the Apex Central server and its managed products, endpoints, or servers.
Administrative responsibility	Group managed products, endpoints, and servers according to system or security personnel assigned to them. This allows group configuration.

Determining the Number of Sites

Determine how many sites your Apex Central deployment will cover. You need this information to determine the number of servers to install, as well as where to install the servers.

Gather this information from your organization's WAN or LAN topology charts.

Determining the Number of Managed Products and Endpoints

You also need to know the total number of managed products, and endpoints Apex Central server will manage. Trend Micro recommends gathering managed product, and endpoint population data per site. If you cannot get this information, even rough estimates will be helpful. You will need this information to determine how many servers to install.

Planning for the Optimal Ratio of Server to Managed Products

When deploying Apex Central across a WAN, the Apex Central server in the main office administers managed products, endpoints, and other servers in remote offices. Managed products, endpoints, or servers in remote offices may require different network bandwidth when communicating with the Apex Central server over a WAN. Apex Central prioritizes communication with the managed products, endpoints, or servers with the faster connections.

Use the recommended system requirements as a guide in determining the CPU and RAM requirements for your Apex Central network.

Designating Apex Central Servers

Based on the number of managed products and endpoints, decide and designate your Apex Central server.

Locate your Windows servers, and then select the ones to assign as Apex Central servers. You also need to determine if you need to install a dedicated server.

When selecting a server that will host Apex Central, consider the following:

- The CPU load
- Other functions the server performs

If you are installing Apex Central on a server that has other uses (for example, application server), Trend Micro recommends installing on a server that does not run mission-critical or resource-intensive applications.

Deciding Where to Install the Apex Central Server

Once you know the number of clients and the number of servers you need to install, find out where to install your Apex Central servers. Decide if you need to install all your servers in the central office or if you need to install some of them in remote offices.

Place the servers strategically in certain segments of your environment to speed up communication and optimize managed product, endpoint, and server management:

- **Central office**: A central office is the facility where the majority of the managed products, endpoints, and servers in the organization are located. The central office is sometimes referred to as headquarters, corporate office, or corporate headquarters. A central office can have other smaller offices or branches (referred to as "remote offices" in this guide) in other locations.

  Tip

  Trend Micro recommends installing a server in the central office.

- **Remote office**: A remote office is defined as any small professional office that is part of a larger organization and has a WAN connection to the central office. If you have managed products, endpoints, and servers in a remote office that report to the server in the central office, they may encounter difficulties connecting to the server. Bandwidth limitations may prevent proper communication to and from the Apex Central server.

  The network bandwidth between your central office and remote office may be sufficient for routine client-server communication, such as notifications for updated configuration settings and status reporting, but insufficient for deployment and other tasks.

Planning for Network Traffic

Apex Central generates network traffic when the server and managed products/endpoints communicate. Plan the Apex Central network traffic to minimize the impact on an organization's network.

These are the sources of Apex Central-related network traffic:

- Heartbeat
- Logs

- Managed product registration to Apex Central server

  Apex Central servers, by default, contain all the product profiles available during the Apex Central release. However, if you register a new version of a product to Apex Central, a version that does not correspond to any existing product profiles, the new product will upload its profile to the Apex Central server.

  For brand-new Trend Micro products that have not had a product profile, Trend Micro delivers updates to enable Apex Central to identify these products.

- Downloading and deploying updates
- Policy deployment
- Suspicious object synchronization

Apex Central Setup Flow

Setting up your Apex Central system is a multi-step process that involves the following:

1. Planning the Apex Central system installation (server distribution, network traffic, data storage, and web server considerations).
2. Installing the Apex Central server.

Note

During installation of the Apex Central server, provide a location for backup and restoration files.

Testing Apex Central at One Location

A pilot deployment provides an opportunity for feedback to determine how features work and the level of support likely needed after full deployment.

Tip

Trend Micro recommends conducting a pilot deployment before performing a full-scale deployment.

Piloting Apex Central at one location allows you to accomplish the following:

- Gain familiarity with Apex Central and managed products
- Develop or refine the company's network policies

A pilot deployment is useful to determine which configurations need improvements. It gives the IT department or installation team a chance to rehearse and refine the deployment process and to verify that your deployment plan meets your organization's business requirements.

A Apex Central test deployment consists of the following tasks:

- Preparing for the test deployment
- Selecting a test site
- Beginning the test deployment
- Evaluating the test deployment

Preparing for the Test Deployment

Complete the following activities during the preparation stage.

Procedure

1. Decide the Apex Central server and agent configuration for the test environment.
    - Establish TCP/IP connectivity among all systems in a trial configuration.
    - Verify bidirectional TCP/IP communications by sending a ping command to each agent system from the manager system and vice versa.

2. Evaluate the different deployment methods to see which ones are suitable for your particular environment.
3. Complete a System Checklist used for the pilot deployment.

Selecting a Test Site

Select a pilot site that best matches your production environment. Try to simulate, as closely as possible, the type of topology that would serve as an adequate representation of your production environment.

Beginning the Test Deployment

After completing the preparation steps and System Checklist, begin the pilot deployment by installing the Apex Central server and agents.

Evaluating the Test Deployment

Create a list of successes and failures encountered throughout the pilot process. Identify potential *pitfalls* and plan accordingly for a successful deployment.

You can implement the pilot evaluation plan into the overall production installation and deployment plan.

Server Distribution Plan

Consider the following when planning for server distribution:

- Administration models
- Apex Central server distribution
- Single-server topology

- Multiple-server topology

Understanding Administration Models

Early in the Apex Central deployment, determine exactly how many people you want to grant access to your Apex Central server. The number of users depends on how centralized you want your management to be. The guiding principle being: the degree of centralization is inversely proportional to the number of users.

Follow one of these administration models:

- **Centralized management**: This model gives Apex Central access to as few people as possible. A highly centralized network would have only one administrator, who then manages all the antivirus and content security servers on the network.

  Centralized management offers the tightest control over your network antivirus and content security policy. However, as network complexity increases, the administrative burden may become too much for one administrator.

- **Decentralized management**: This is appropriate for large networks where system administrators have clearly defined and established areas of responsibility. For example, the mail server administrator may also be responsible for email protection; regional offices may be independently responsible for their local areas.

  A main Apex Central administrator would still be necessary, but he or she shares the responsibility for overseeing the network with other product or regional administrators.

  Grant Apex Central access to each administrator, but limit access rights to view and/or configure segments of the Apex Central network that are under their responsibility.

With one of these administration models initialized, you can then configure the Product Directory and necessary user accounts to manage your Apex Central network.

Understanding Apex Central Server Distribution

Apex Central can manage products regardless of physical location, and so it is possible to manage all your antivirus and content security products using a single Apex Central server.

However, there are advantages to dividing control of your Apex Central network among different servers. Based on the uniqueness of your network, you can decide the optimum number of Apex Central servers.

Single-Server Topology

The single-server topology is suitable for small to medium, single-site enterprises. This topology facilitates administration by a single administrator, but does not preclude the creation of additional administrator accounts as required by your Administration plan.

However, this arrangement concentrates the burden of network traffic (agent polling, data transfer, update deployment, and so on) on a single server, and the LAN that hosts it. As your network grows, the impact on performance also increases.

Multiple-Server Topology

For larger enterprises with multiple sites, it may be necessary to set up regional Apex Central servers to divide the network load.

For information on the traffic that a Apex Central network generates, see *Understanding Apex Central Network Traffic on page 2-14*.

Network Traffic Plan

To develop a plan to minimize the impact of Apex Central on your network, it is important to understand the network traffic generated by Apex Central.

The following section helps you understand the traffic that your Apex Central network generates and develop a plan to minimize its impact on your network. In addition, the section about traffic frequency describes which sources frequently generate traffic on a Apex Central network.

Understanding Apex Central Network Traffic

To develop a plan to minimize the impact of Apex Central on your network, it is important to understand the network traffic generated by Apex Central.

Sources of Network Traffic

The following Apex Central sources generate network traffic:

- Log traffic
- MCP policies
- Product registration
- Downloading and deploying updates
- Deploying policy settings

Traffic Frequency

The following sources frequently generate traffic on a Apex Central network:

- Logs generated by managed products
- MCP polling and commands

Logs

Managed products send logs to Apex Central at different intervals, depending on their individual log settings.

Managed Product Agent Heartbeat

By default, managed product agents send heartbeat messages every 60 minutes. Administrators can adjust this value from 5 to 480 minutes (8 hours). When choosing a heartbeat setting, choose a balance between the need to display the latest status information and the need to manage system resources.

The default setting will be satisfactory for most situations, however should you feel the need to customize these settings, consider the following:

- **Long-Interval Heartbeats** (above 60 minutes): The longer the interval between heartbeats, the greater the number of events that may occur before the Apex Central console displays the interval.

  For example, if a connection problem with an agent is resolved between heartbeats, it then becomes possible to communicate with an agent even if its status appears as *Inactive* or *Abnormal*.

- **Short-Interval Heartbeats** (below 60 minutes): Short intervals between heartbeats present a more up-to-date picture of your network status at the Apex Central server. However, short-interval heartbeats increase the amount of network bandwidth used.

> **Note**
>
> Before adjusting the interval to a number below 15 minutes, study your existing network traffic to understand the impact of increased use of network bandwidth.

Network Protocols

Apex Central uses the UDP and TCP protocols for communication.

Source of Network Traffic

Log Traffic

Constant sources of network traffic in a Apex Central network are "product logs", logs that managed products regularly send to the Apex Central server.

TABLE 2-2. Apex Central Log Traffic

LOG	CONTAINS INFORMATION ABOUT
Virus/Spyware/ Grayware	Detected virus/malware, spyware/grayware, and other security threats
Security	Violations reported by content security products
Web Security	Violations reported by web security products
Event	Miscellaneous events (for example, component updates, and generic security violations)
Status	The environment of a managed product. The Status tab of the Product Directory displays this information
Network Virus	Viruses detected in network packets
Performance Metric	Used for previous product versions
URL Usage	Violations reported by web security products
Security Violation	Violations reported by Network VirusWall products.
Security Compliance	Endpoint compliances reported by Network VirusWall products
Security Statistic	The difference between security compliances and security violations calculated and reported by Network VirusWall products.
Endpoint	Violations reported by Web security products.
Data Loss Prevention Log	Detections related to Data Loss Prevention policy violations
Behavior Monitoring Log	Behavior-based malicious activity detections
Network Inspection Log	Includes IP address or domain detections
Predictive Machine Learning Log	Predictive Machine Learning detections
Virtual Analyzer Log	Detections reported by Virtual Analyzer for suspicious sample submissions

Log	Contains Information About
File Hash Detection Log	Detections triggered by **File** or **File SHA-1** suspicious objects

Trend Micro Management Communication Protocol Policies

The Trend Micro Management Communication Protocol (MCP) is the Apex Central communications backbone. MCP implements the following policies:

- **MCP Heartbeat**: The MCP heartbeats to Apex Central ensure that Apex Central displays the latest information and that the connection between the managed product and the Apex Central server is functional.
- **MCP Command Polling**: When an MCP agent initiates a command poll to Apex Central, Apex Central notifies the agent to send managed product logs or issues a command to the managed product. Apex Central also interprets a command poll as a passive heartbeat verifying the connection between Apex Central and the managed product.

Product Registration Traffic

Product profiles provide Apex Central with information about how to manage a particular product. Managed products upload profiles to the Apex Central server the first time they register with the server.

Each product has a corresponding product profile, and in many cases, different versions of a product have their own, version-specific profile. Profiles contain the following information:

- Category (for example, antivirus)
- Product name
- Product version
- Menu version
- Log format

- Update component information – updates that the product supports (for example, virus pattern files)
- Command information

By default, Apex Central servers contain all the product profiles for managed products that use Web Services Integration communication. Managed products that use the Trend Micro Management Communication Protocol (MCP) upload product profiles during initial registration with the Apex Central server.

Policy Deployment

Apex Central generates network traffic when deploying policy settings to managed products and endpoints. The traffic originates from the following sources:

- Periodic policy enforcement

  Apex Central enforces the policy settings on managed products and endpoints every 24 hours.

- Deployed information

  A policy contains the Globally Unique Identifier (GUID) information for each endpoint and the setting information. A policy containing 50,000 targets and a full set of settings can generate up to 1.8MB of network traffic.

Deploying Updates

Updating the Apex Central network is a two-step process:

1. Obtain the latest update components from Trend Micro.

   Apex Central can download components either directly from the Trend Micro update server, or from an alternative location.

2. Deploy these components to the managed products.

   Apex Central deploys update components to managed products, including:

   - Pattern files/Cleanup templates
   - Engines (scan engines, damage cleanup engines)
   - Antispam rules
   - Apex One Plug-in Manager Plug-in Programs
   - Product programs (depending on the product)

   Tip

   Trend Micro strongly recommends regularly updating these components to help ensure managed products can protect your network against the latest threats. For product program updates, refer to the specific program's documentation.

   Deploying updates to managed products is a bandwidth-intensive operation. If possible, it is important to perform deployments when they will have the least impact on the network.

   You can stagger the deployment of component updates using Deployment Plans.

   Furthermore, check that the network connection between your Apex Central server and managed products can accommodate the updates. The connection is a factor to consider when deciding how many Apex Central servers your network needs.

Data Storage Plan

Apex Central data must be stored in an SQL database. When you install Apex Central on a server that does not have its own database, the installation program provides the option to install the Microsoft SQL Express. However, due to the limitations of SQL Express, large networks require an SQL server.

Note

Apex Central uses SQL and Windows authentication to access the SQL server.

Database Recommendations

This section provides recommendations for administrators when installing Apex Central and the SQL server on the same computer.

- Production environment
  - Use a computer with more than 10GB of disk space

    Note

    The minimum disk space requirement to install Apex Central is 10GB, but the recommended requirement is 80GB. Trend Micro recommends at least 80GB of disk space for installing Apex Central and the SQL server on the same computer.

  - Configure the maximum amount of memory used by the SQL server

    Leave at least 8GB of memory for Apex Central and system usage.

    For example, if a computer has 80GB of memory, set the maximum memory usage of the SQL server to 72GB. In this case, 8GB of memory is available for Apex Central and system usage.
- Test environment

  Leave at least 8GB of memory for Apex Central and system usage.

Note

For details on how to configure memory usage for the SQL server, see https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/server-memory-server-configuration-options.

Tip

- For Apex Central managing more than 1,000 products (including Apex One Security Agents and ServerProtect Normal servers), Trend Micro recommends using a dedicated SQL server.
- If Apex Central and the SQL server are installed on different computers, set the same time zone on both computers.
- Trend Micro highly recommends using Microsoft SQL Server Standard or Enterprise Edition. SQL Express is suitable for testing purposes but not for production environments.

ODBC Driver

Apex Central installs Open Database Connectivity (ODBC) Driver 13 for SQL Server to support Microsoft SQL Server communications and Transport Layer Security (TLS) 1.2.

Authentication

Apex Central supports both SQL database authentication and Windows authentication.

Web Server Plan

The web server information screen in the Apex Central setup program presents similar server identification options as the host ID definition screen: host name, FQDN, or IP address. The decision considerations for the web server name are the same:

- Using the host name or FQDN facilitates Apex Central server IP address changes, but makes the system dependent on the DNS server
- The IP address option requires a fixed IP

Use the web server address to identify the source of component updates. The `SystemConfiguration.xml` file stores this information and sends it to agents as part of a notification for these agents to obtain updates from the Apex Central server. Update source related settings appear as follows:

```
Value=http://Web server address>:port>/TvcsDownload/
ActiveUpdate/component>
```

Where:

- **Port**: The port that connects to the update source. You can also specify this on the web server address screen (default port number is 80)
- **TvcsDownload/ActiveUpdate**: The Apex Central setup program creates this virtual directory in the IIS-specified website
- **Component**: This depends on the updated component. For example, when the virus pattern file is updated, the value added here is:

  ```
  Pattern/vsapi.zip
  ```

  `Pattern` corresponds to the `\\. . . Control Manager\WebUI \download\activeupdate\pattern` folder on the Apex Central server. `Vsapi.zip` is the virus pattern in compressed form.

Chapter 3

Installation

This chapter guides you through installing the Apex Central server. The chapter also contains post-installation configuration information as well as instructions on how to register and activate your software.

Topics include:

- *System Requirements on page 3-2*
- *Installing the Apex Central Server on page 3-8*

System Requirements

Apex Central runs on Windows Server and requires specific Windows features and hotfixes in order to install. Apex Central also requires a supported version of Microsoft SQL Server, at least 8 GB of RAM, and at least 10 GB of available disk space.

- For complete system requirements and supported Windows Server and Microsoft SQL Server versions, download the *Apex Central System Requirements* document from http://docs.trendmicro.com/en-us/enterprise/apex-central.aspx.
- For detailed managed product and Security Agent system requirements, see the managed product documentation.

The following tables list the minimum Windows Server requirements for running the Apex Central installation program.

- *Windows Server 2012 on page 3-3*
- *Windows Server 2012 R2 on page 3-4*
- *Windows Server 2016 on page 3-5*
- *Windows Server 2019 on page 3-6*
- *Windows Server 2022 on page 3-7*

Note

- The following Windows hotfixes are not automatically installed by Windows Updates but are required for the respective operating systems prior to Apex Central installation:
    - KB2999226
    - KB2919355
    - KB2919442
- The following Windows hotfixes are only required for the respective operating systems to support TLS 1.2:
    - KB2975331
    - KB3000850

TABLE 3-1. Windows Server 2012

ITEM	REQUIREMENT
Editions (no Service Pack required)	• Standard • Datacenter
Processor	• At least 2.3 GHz Intel™ Core™ i5 or compatible CPUs • AMD™ 64 processor • Intel™ 64 processor
RAM	• 8 GB minimum
Available Disk Space	• 10 GB minimum • 80 GB recommended (SAS)

Item	Requirement
Windows Features	• Microsoft IIS 8.0 • Microsoft IIS Windows Authentication • Microsoft IIS ASP • Microsoft IIS ASP.NET 4.5 • Microsoft IIS ASP.NET Extensibility 4.5 • Microsoft IIS CGI • Microsoft Message Queuing Service (MSMQ)
Windows Hotfixes	• KB2999226 • KB2975331

Table 3-2. Windows Server 2012 R2

Item	Requirement
Editions (no Service Pack required)	• Standard • Datacenter
Processor	• At least 2.3 GHz Intel™ Core™ i5 or compatible CPUs • AMD™ 64 processor • Intel™ 64 processor
RAM	• 8 GB minimum
Available Disk Space	• 10 GB minimum • 80 GB recommended (SAS)

ITEM	REQUIREMENT
Windows Features	• Microsoft IIS 8.5 • Microsoft IIS Windows Authentication • Microsoft IIS ASP • Microsoft IIS ASP.NET 4.5 • Microsoft IIS ASP.NET Extensibility 4.5 • Microsoft IIS CGI • Microsoft Message Queuing Service (MSMQ)
Windows Hotfixes	• KB2919355 • KB2919442 • KB3000850

TABLE 3-3. Windows Server 2016

ITEM	REQUIREMENT
Editions (no Service Pack required)	• Standard • Datacenter
Processor	• At least 2.3 GHz Intel™ Core™ i5 or compatible CPUs • AMD™ 64 processor • Intel™ 64 processor
RAM	• 8 GB minimum
Available Disk Space	• 10 GB minimum • 80 GB recommended (SAS)

ITEM	REQUIREMENT
Windows Features	- Microsoft IIS 10.0 - Microsoft IIS Windows Authentication - Microsoft IIS ASP - Microsoft IIS ASP.NET 4.6 - Microsoft IIS ASP.NET Extensibility 4.6 - Microsoft IIS CGI - Microsoft Message Queuing Service (MSMQ)
Windows Hotfixes	- N/A

TABLE 3-4. Windows Server 2019

ITEM	REQUIREMENT
Editions (no Service Pack required)	- Standard - Datacenter
Processor	- At least 2.3 GHz Intel™ Core™ i5 or compatible CPUs - AMD™ 64 processor - Intel™ 64 processor
RAM	- 8 GB minimum
Available Disk Space	- 10 GB minimum - 80 GB recommended (SAS)

Item	Requirement
Windows Features	• Microsoft IIS 10.0 • Microsoft IIS Windows Authentication • Microsoft IIS ASP • Microsoft IIS ASP.NET 4.7 • Microsoft IIS ASP.NET Extensibility 4.7 • Microsoft IIS CGI • Microsoft Message Queuing Service (MSMQ)
Windows Hotfixes	• N/A

Table 3-5. Windows Server 2022

Item	Requirement
Editions (no Service Pack required)	• Standard • Datacenter
Processor	• At least 2.3 GHz Intel™ Core™ i5 or compatible CPUs • AMD™ 64 processor • Intel™ 64 processor
RAM	• 8 GB minimum
Available Disk Space	• 10 GB minimum • 80 GB recommended (SAS)

Item	Requirement
Windows Features	- Microsoft IIS 10.0 - Microsoft IIS Windows Authentication - Microsoft IIS ASP - Microsoft IIS ASP.NET 4.8 - Microsoft IIS ASP.NET Extensibility 4.8 - Microsoft IIS CGI - Microsoft Message Queuing Service (MSMQ)
Windows Hotfixes	- N/A

Installing the Apex Central Server

After deciding on the topology to use for your network, you can begin to install your Apex Central server.

See *Server Address Checklist on page 8-2* to help you record relevant information for installation.

You need the following information for the installation:

- Relevant target server address and port information
- Apex Central Registration Key
- Security Level to use for Server-Agent communication

The following are database-related considerations:

- Decide if you want to use an SQL server with Apex Central. If the SQL server is located on a server other than the Apex Central server, obtain its IP address, FQDN, or NetBIOS name. If there are multiple instances of the SQL server, identify the one that you intend to use
- Prepare the following information about the SQL database for Apex Central:

  - User name for the database
  - Password

> **Note**
>
> Apex Central allows you to use Windows authentication or SQL authentication to access the SQL server.

- Determine the number of managed products that Apex Central will handle. If an SQL server is not detected on the server, Apex Central installs SQL Server 2017 Express, which can only handle a limited number of connections

Apex Central Installation Flow

Installing Apex Central requires performing the following steps:

1. Install all required components
2. Specify the installation location
3. Register and activate the product and services
4. Specify the backup settings
5. Set up the root account
6. Configure database information

> **Tip**
>
> Trend Micro recommends upgrading to the latest version of Apex Central instead of doing a fresh installation.

Installing All Required Components

Procedure

1. Run the Apex Central installation program (`Trend Micro Apex Central.exe`) on the server.

   The installation program checks your system for required components.

   - If .NET Framework 4.6.1 or above is not already installed, proceed to step 2.
   - If .NET Framework 4.6.1 or above is already installed, skip to step 3.

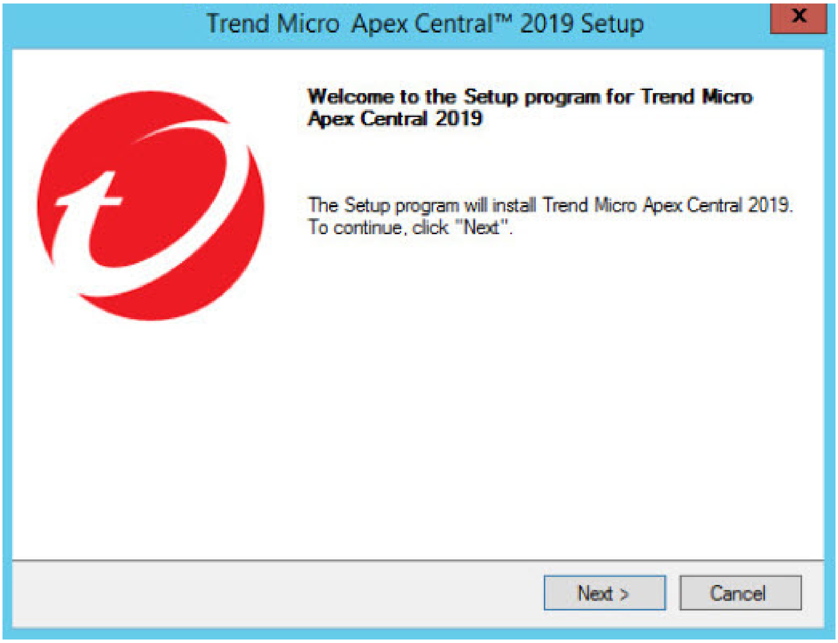
2. Click **Accept and Install** to accept the Microsoft license terms and install the framework.

   The installation program installs .NET Framework 4.6.1.

   > **Note**
   >
   > You may need to restart the server to after installing the missing component.

3. Click **Yes** to continue the installation.

The **Welcome** screen appears.



Trend Micro Apex Central™ 2019 Setup

Welcome to the Setup program for Trend Micro Apex Central 2019

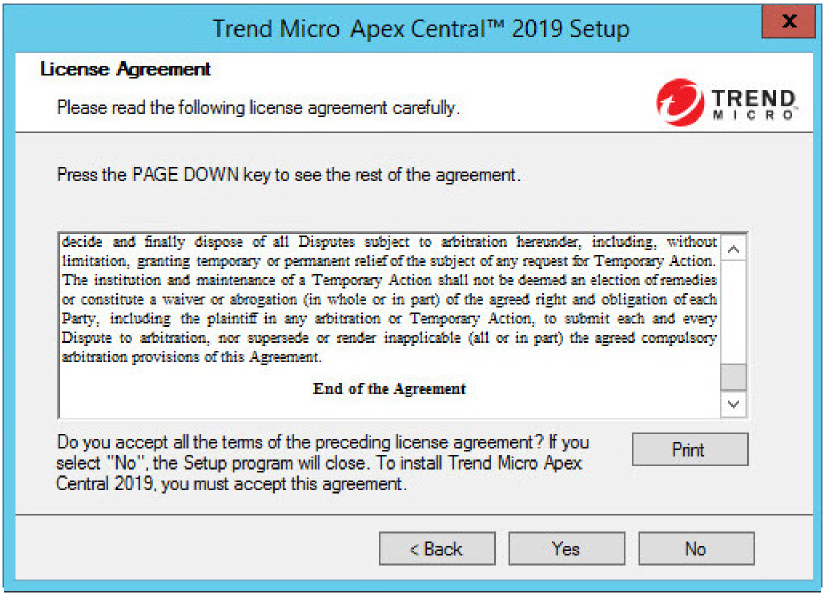
The Setup program will install Trend Micro Apex Central 2019. To continue, click "Next".

FIGURE 3-1. The Welcome screen

The installation program checks your system for existing components. Before proceeding with the installation, close all instances of the **Microsoft Management Console**.

4. Click **Next**.

The **Software License Agreement** screen appears.



License Agreement

Please read the following license agreement carefully.

Press the PAGE DOWN key to see the rest of the agreement.

decide and finally dispose of all Disputes subject to arbitration hereunder, including, without limitation, granting temporary or permanent relief of the subject of any request for Temporary Action. The institution and maintenance of a Temporary Action shall not be deemed an election of remedies or constitute a waiver or abrogation (in whole or in part) of the agreed right and obligation of each Party, including the plaintiff in any arbitration or Temporary Action, to submit each and every Dispute to arbitration, nor supersede or render inapplicable (all or in part) the agreed compulsory arbitration provisions of this Agreement.

End of the Agreement

Do you accept all the terms of the preceding license agreement? If you select "No", the Setup program will close. To install Trend Micro Apex Central 2019, you must accept this agreement.

FIGURE 3-2. Agree with the License Agreement

5. Read the terms of the license agreement and choose one of the following:

    - If you do not agree with the terms of the license, click **No**.

      The installation stops.

    - To proceed with the installation, click **Yes**.

      The **Local System Environment Analysis Screen** appears.

Note

If a SQL server database is not already installed, the installation program will install Microsoft SQL Server 2017 Express at the end of the procedure.

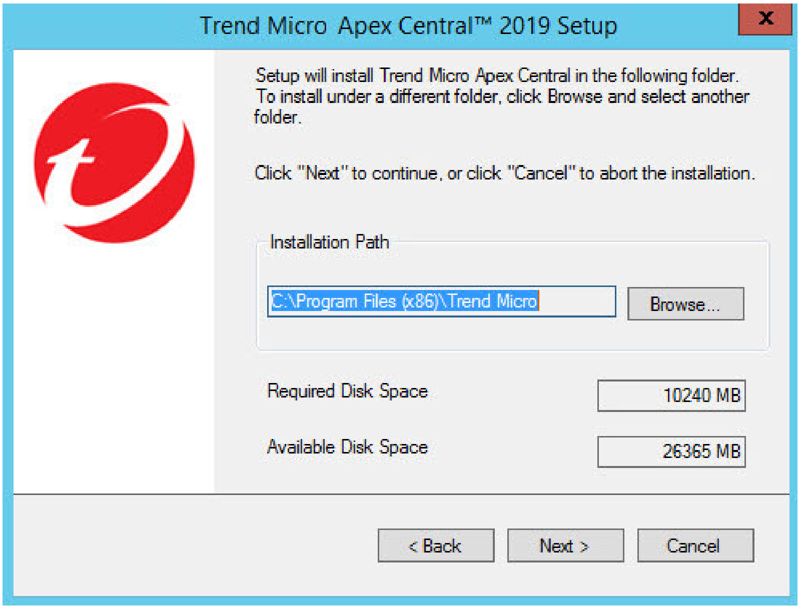
For more information, see *Configuring Database Information on page 3-20*.

Specifying the Installation Location

Procedure

1. Click **Next**.

   The **Select Destination Folder** screen appears.



Trend Micro Apex Central™ 2019 Setup

Setup will install Trend Micro Apex Central in the following folder. To install under a different folder, click Browse and select another folder.

Click "Next" to continue, or click "Cancel" to abort the installation.

Installation Path

C:\Program Files (x86)\Trend Micro

Required Disk Space: 10240 MB

Available Disk Space: 26365 MB

FIGURE 3-3. Select a destination folder

2. Specify a location for Apex Central files. Click **Browse** to specify an alternate location.

   Note

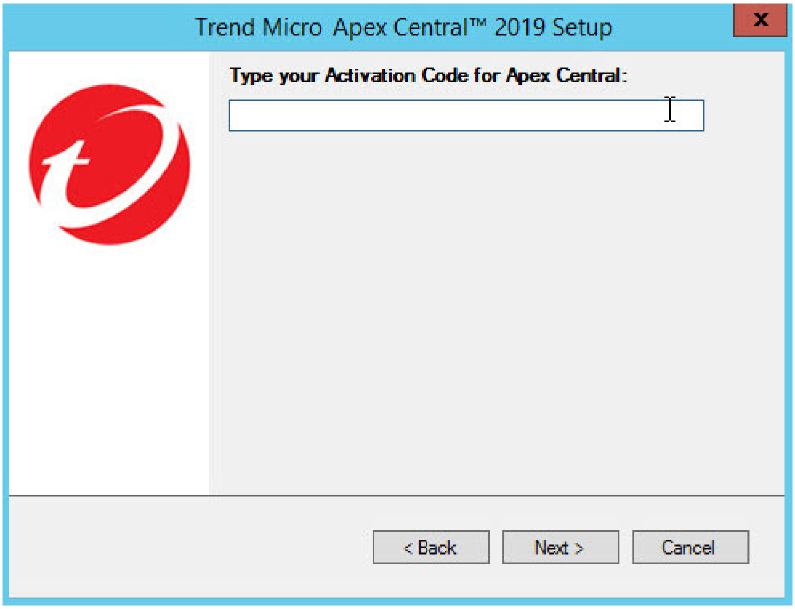
   - The default location on 64-bit operating systems is `C:\Program Files (x86)\Trend Micro`.
   - The setup program installs files related to Apex Central communication (MCP) in predetermined folders in the `Program Files` folder.

Activating the Product and Services

Procedure

1. Click **Next**.

The **Product Activation** screen appears.



Type your Activation Code for Apex Central:

FIGURE 3-4. Provide the Activation Code to activate and services

2. Type the Apex Central Activation Code in the space provided.

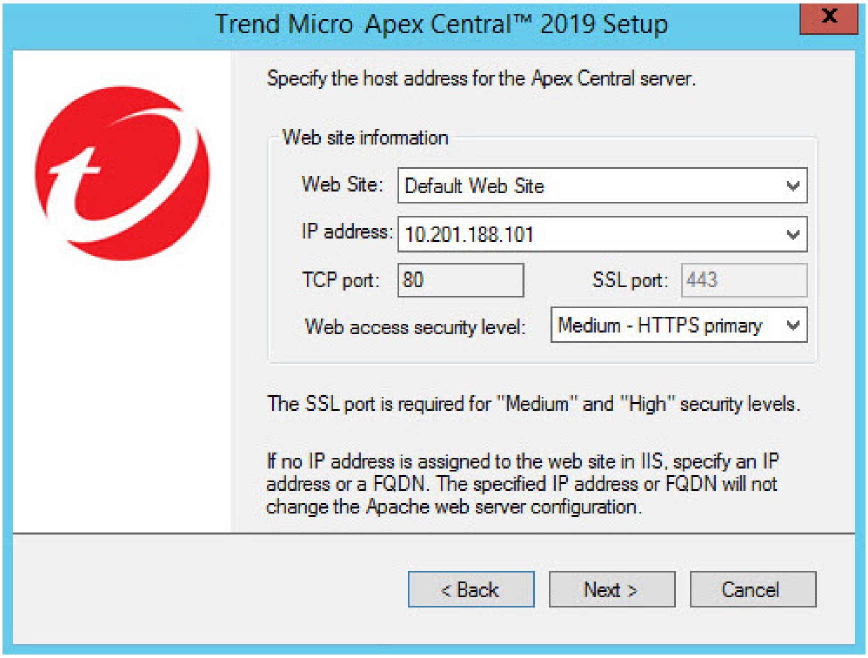
Specifying Apex Central Web Server Settings

Procedure

1. Click **Next**.

   The **Specify Web Server Information** screen appears.

The settings on the **Specify Web Server Information** screen define communication security and how the Apex Central network identifies your server.



Trend Micro Apex Central™ 2019 Setup

Specify the host address for the Apex Central server.

Web site information

Web Site: Default Web Site

IP address: 10.201.188.101

TCP port: 80

SSL port: 443

Web access security level: Medium - HTTPS primary

The SSL port is required for "Medium" and "High" security levels.

If no IP address is assigned to the web site in IIS, specify an IP address or a FQDN. The specified IP address or FQDN will not change the Apache web server configuration.

FIGURE 3-5. Specify web server information

2. From the **Web site** list, select the website to access Apex Central.

3. From the IP address list, select the FQDN/host name, IPv4, or IPv6 address you want to use for the Apex Central Management Console. This setting defines how the Apex Central communication system identifies your Apex Central server. The setup program attempts to detect both the server's fully qualified domain name (FQDN) and IP address and displays them in the appropriate field.

   If your server has more than one network interface card, or if you assign your server more than one FQDN, the names and IP addresses appear here. Choose the most appropriate address or name by selecting the corresponding option or item in the list.

If you use the host name or FQDN to identify your server, make sure that this name can be resolved on the product computers; otherwise the products cannot communicate with the Apex Central server.

4. From the **Web access security level** list, select one of the following security security levels for Apex Central communication:

   - **High - HTTPS only**: All Apex Central communication uses HTTPS protocol. This ensures the most secure communication between Apex Central and other products.

   - **Medium - HTTPS primary**: If supported all Apex Central communication uses HTTPS protocol. If HTTPS is unavailable, agents use HTTP instead. This is the default setting when installing Apex Central.

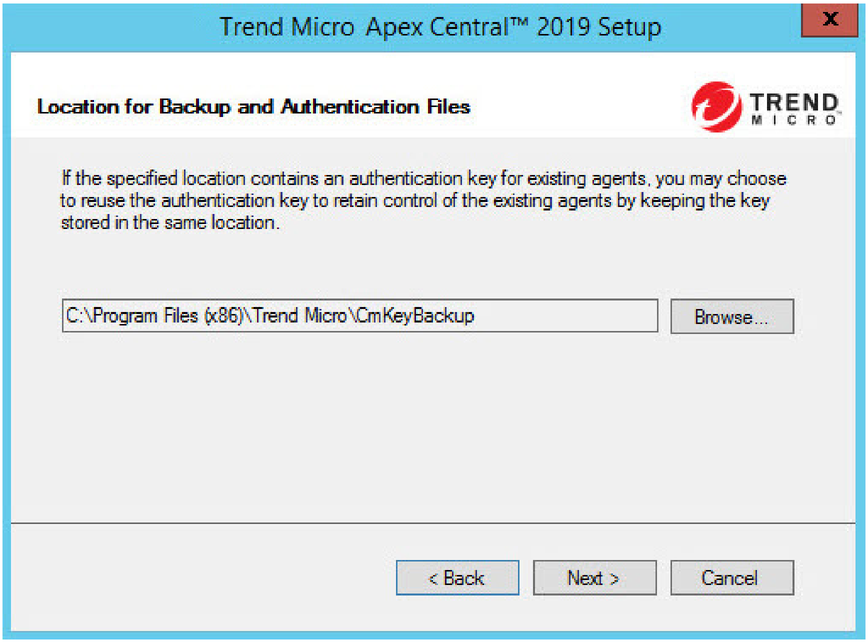
   - **Low - HTTP based**: All Apex Central communication uses HTTP protocol. This is the least secure communication method between Apex Central and other products.

Specifying Backup Settings

Procedure

1. Click **Next**.

The **Choose Destination Location** screen appears.



Trend Micro Apex Central™ 2019 Setup

Location for Backup and Authentication Files

If the specified location contains an authentication key for existing agents, you may choose to reuse the authentication key to retain control of the existing agents by keeping the key stored in the same location.

C:\Program Files (x86)\Trend Micro\CmKeyBackup

FIGURE 3-6. Choose a destination location for backup and authentication files

2. Specify the location of the Apex Central backup and authentication files. Click **Browse** to specify an alternate location.

Note

The default location on 64-bit operating systems is `C:\Program Files (x86)\Trend Micro\CmKeyBackup`.

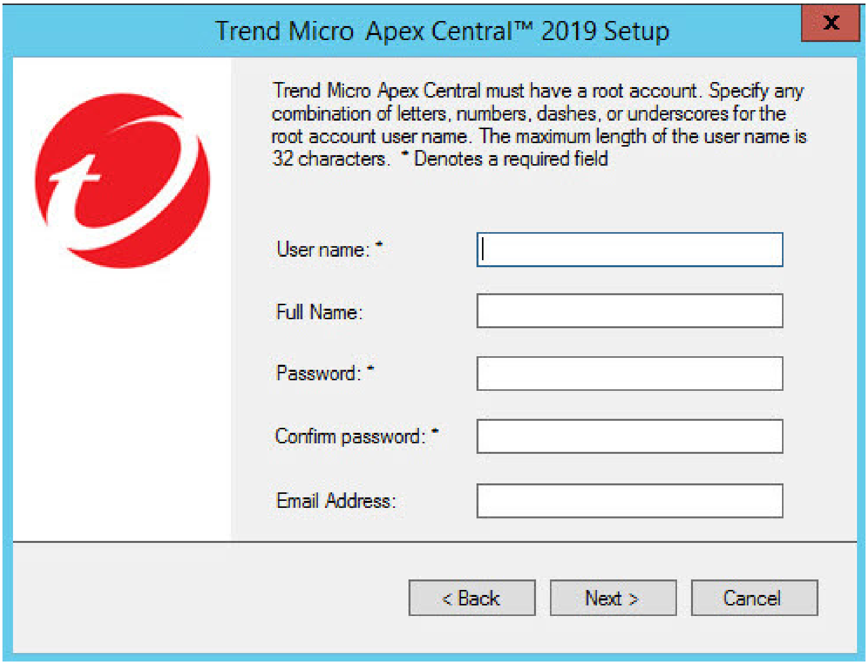
For more information, see *Server Files to Back Up Before Migration on page 5-3*.

Setting Up the Root Account

Procedure

1. Click **Next**.

   The following screen appears.



Trend Micro Apex Central™ 2019 Setup

Trend Micro Apex Central must have a root account. Specify any combination of letters, numbers, dashes, or underscores for the root account user name. The maximum length of the user name is 32 characters. * Denotes a required field

User name: *

Full Name:

Password: *

Confirm password: *

Email Address:

FIGURE 3-7. Provide information for the Apex Central root account

2. Provide the following account information:

   - **User name** (required)
   - **Full name**
   - **Password** (required)

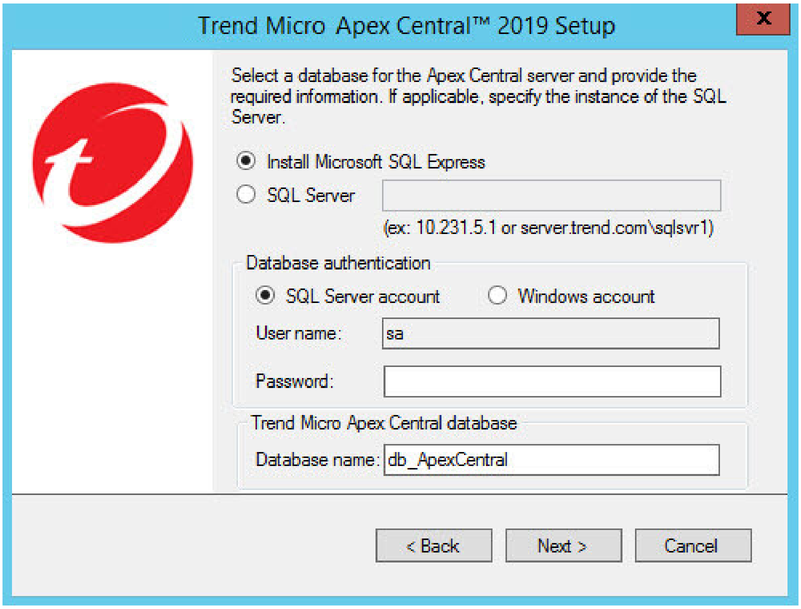
- **Confirm password** (required)
- **Email address**

Configuring Database Information

Procedure

1. Click **Next**.

   The **Setup Apex Central Database** screen appears.



Trend Micro Apex Central™ 2019 Setup

Select a database for the Apex Central server and provide the required information. If applicable, specify the instance of the SQL Server.

● Install Microsoft SQL Express

○ SQL Server

(ex: 10.231.5.1 or server.trend.com\sqlsvr1)

Database authentication

● SQL Server account ○ Windows account

User name: sa

Password:

Trend Micro Apex Central database

Database name: db_ApexCentral

FIGURE 3-8. Choose the Apex Central database

2. Select a database to use with Apex Central.

   - **Install Microsoft SQL Express**: The setup program automatically selects this option if an SQL server is not installed on this computer.

Do not forget to specify a password for this database in the field provided.

Tip

Microsoft SQL Server Express is suitable only for a small number of connections. Trend Micro recommends using an SQL server for large Apex Central networks.

- **SQL Server**: The setup program automatically selects this option if the program detects an SQL server on the server. Provide the following information:

  - **SQL Server (\Instance)**: This server hosts the SQL server that you want to use for Apex Central. If an SQL server is present on your server, the setup program automatically selects it.

    To specify an alternative server, identify it using its FQDN, IPv4 address, or NetBIOS name.

    If more than one instance of SQL server exists on a host server (this can be either the same server where you are installing Apex Central, or another server), you must specify the instance. For example: `your_sql_server.com\instance`

    Note

    If users choose to use a remote SQL server, do not specify an IPv6 address in the SQL Server field. Apex Central cannot identify the remote database by its IPv6 address.

3. Provide credentials to access the SQL server in **Database authentication**.

WARNING!

For security reasons, do not use an SQL database that is not password protected.

Important

Both the **SQL Server Account** and **Windows Account** should meet the following requirements:

- Belongs to the “Administrators Group”
- Contains the “Log on as a service” user right
- Contains the “db_creator” or “db_owner” database roles
  - The “db_creator” role is required if creating a new database (the target database does not already exists).
  - The “db_owner” role is sufficient if the target database already exists.

Tip

If using an existing database, Trend Micro strongly recommends preparing an empty database for Apex Central installation.

- **SQL Server Account**

  By default, the user name is **sa**.

- **Windows Account**

  Type the user name in the following format: `domain name\user name`.

4. Under **Trend Micro Apex Central database**, provide a name for the Apex Central database.

   The default name is db_ApexCentral.

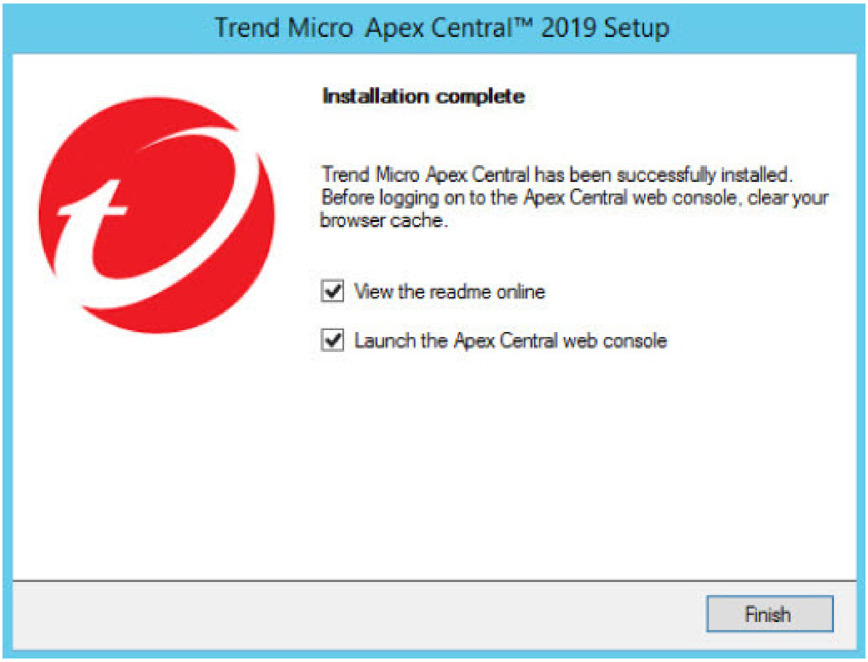
5. Click **Next** to create the required database. If the setup program detects an existing Apex Central database, you have the following options:

   - **Delete existing records, and create a new database**: The existing database is deleted, and another is created using the same name.

- **Create a new database with a new name**: You are returned to the previous screen to allow you to change your Apex Central database name.

6. Click **Next**.

7. Click **Finish** to complete the installation.



Trend Micro Apex Central™ 2019 Setup

Installation complete

Trend Micro Apex Central has been successfully installed. Before logging on to the Apex Central web console, clear your browser cache.

☑ View the readme online

☑ Launch the Apex Central web console

FIGURE 3-9. Setup complete

Chapter 4

Post-installation Tasks

This chapter discusses the tasks Trend Micro recommends performing after the Apex Central installation completes.

Topics include:

- *Automatic Post-installation Tasks on page 4-2*
- *Verifying the Server Installation or Upgrade on page 4-2*
- *Activating Your Software on page 4-4*
- *Configuring Active Directory Connection Settings on page 4-5*
- *Configuring User Accounts on page 4-8*
- *Downloading the Latest Components on page 4-8*
- *Configuring Event Notifications on page 4-9*

Automatic Post-installation Tasks

Apex Central automatically performs the following tasks after successfully upgrading or migrating from Control Manager 6.0 Service Pack 3 Patch 3.

- Migrate previously configured Active Directory server settings
- Synchronize Active Directory server data

Verifying the Server Installation or Upgrade

After completing the installation or upgrade, verify the following items:

Item	Description
Programs list	The following programs appear on the **Add/Remove Programs** list (**Control Panel** > **Add/Remove Programs**) on the server computer: • Trend Micro Apex Central • Microsoft Visual C++ 2005, 2008, 2012, 2015 Redistributable • Microsoft Report Viewer 2012 Runtime • Microsoft SQL Server 2017 • Microsoft SQL Server 2017 Native Client • Microsoft SQL Server 2017 Setup • Microsoft SQL Server 2017 Setup Support Files • Microsoft SQL Server Browser • Microsoft SQL Server VSS Writer
Directory folders	The following folders appear in the `C:\Program Files (x86)` directory on the server computer: • `Trend Micro\CmKeyBackup` • `Trend Micro\COMMON\TMI` • `Trend Micro\Control Manager`

Item	Description
Apex Central Database files	- `db_ApexCentral.mdf` - `db_ApexCentral_Log.LDF`
The setup program creates the following services and processes:	
Apex Central services	- Trend Micro Apex Central - Trend Micro Management Infrastructure
IIS process	- `w3wp.exe` (Internet Information Services)
ISAPI filters	- ReverseProxy - TmcmRedirect
Apex Central processes	- `CasProcessor.exe` - `CMEFScheduler.NET.exe` - `CmdProcessor.exe` - `CmdProcessor.NET.exe` - `LogForwarder.exe` - `LogProcessor.exe` - `LogReceiver.exe` - `LogRetriever.exe` - `MDRProcessor.NET.exe` - `MsgReceiver.exe` - `ProcessManager.exe` - `ReportServer.exe` - `sCloudProcessor.NET.exe` - `TICAgentForMDR.exe`

Activating Your Software

Activating Apex Central allows you to use all of the product features, including downloading updated program components.

For more information, see the following topics:

- *Activating Apex Central on page 4-4*
- *Converting to the Full Version on page 4-5*

Activating Apex Central

The **License Management** screen allows you to activate Apex Central after obtaining an Activation Code from your Trend Micro sales representative or reseller.

If you purchased a license for Apex One Sandbox as a Service, you can also activate the license from the **License Management** screen.

Important

After activating Apex Central, log off and then log on to the Apex Central web console for changes to take effect.

Procedure

1. Go to **Administration** > **License Management** > **Apex Central**.

   The **License Information** screen appears and displays the current license information.

2. Click the **Specify a new Activation Code** link.
3. Type your Activation Code.
4. Click **Activate**.

5. Log off and then log on to the Apex Central web console for the changes to take effect.

Converting to the Full Version

Activate your Apex Central to continue to use it beyond the evaluation period. Activate Apex Central to use its full functionality including downloading updated program components.

Procedure

1. Purchase a full version Registration Key from a Trend Micro reseller.
2. Register your software online.
3. Obtain an Activation Code.
4. Activate Apex Central according to the instructions in the procedure above.

Configuring Active Directory Connection Settings

Specify the connection settings to allow Apex Central to synchronize endpoint and user information from Active Directory servers.

Note

Apex Central supports synchronization with multiple Active Directory forests. Adding an Active Directory domain automatically synchronizes all domains from the same forest.

For more information about forest trusts, contact your Active Directory administrator.

Procedure

1. Go to **Administration** > **Settings** > **Active Directory and Compliance Settings**.
2. Click the **Active Directory Settings** tab.
3. Select **Enable Active Directory synchronization and authentication**.
4. Configure the connection settings to access an Active Directory server.

FIELD	DESCRIPTION
Server address	Type the FQDN or IP address (IPv4 or IPv6) of the Active Directory server.
User name	Type the domain name and user name required to access the Active Directory server. Example format, `domain\user_name`
Password	Type the password required to access the Active Directory server.

- To add another Active Directory server, click the add icon (+).
- To delete an Active Directory server, click the delete icon (−).

5. From the **Synchronization frequency (in hours)** drop-down list, select how often Apex Central synchronizes data with Active Directory servers.

Note

Active Directory synchronization times vary based on the size and complexity of the Active Directory database. You may need to wait for more than an hour before synchronization completes.

6. (Optional) Expand **Advanced settings** to configure the **Synchronization source** or **Connection mode**.

   a. Select one of the following synchronization sources:

      - **Domain controllers**: Synchronizes all domains from multiple forests with trust relationships

- **Global catalog**: Synchronizes all domains from a single forest

> **Important**
>
> Some information used by Apex Central, such as geographic location and user membership in global groups or domain local groups, cannot be synchronized from a global catalog with default settings. Choose to synchronize from a global catalog only if your network policy restricts Apex Central from connecting to all domain controllers.

b. Select one of the following connection modes:

- **SSL**

> **Important**
>
> To use an SSL connection, import the Active Directory Certificate to the Apex Central server.

- **Non-SSL**

7. (Optional) Click **Test Connection** to test the server connection.

> **Note**
>
> Testing the connection does not save the Active Directory server settings.

The Active Directory server connection status icon (✓ or ✗) appears in front of the server address.

8. Click **Save**.

Apex Central synchronizes endpoint and user information from the Active Directory server(s) according to the synchronization frequency.

9. (Optional) Configure which Active Directory domains and OUs Apex Central synchronizes by modifying the `ADSyncOUList.config` configuration file located at:

```
<Apex Central installation directory>\ADSyncOUList.config
```

10. (Optional) Click **Synchronize Now** to manually synchronize Active Directory data.

    The Active Directory server connection status icon (✓ or ✖) appears in front of the server address.

11. To remove a synchronized Active Directory server:

    a. Clear the **Enable Active Directory synchronization** check box.

    b. Click **Clear Data** to purge the Apex Central server of data from the removed Active Directory server.

       Apex Central removes the synchronized Active Directory server.

       > **Note**
       >
       > Clicking **Clear Data** triggers a scheduled task, which runs every 2 minutes, to purge all data of the removed Active Directory servers from the Apex Central database.

Configuring User Accounts

Create Apex Central user accounts based on your needs. Consider the following when creating your accounts:

- The number of different user roles (Administrators, Power Users, and Operators)
- Assign appropriate permissions and privileges to each user role
- For users to take advantage of the more advanced functions, they need to have Power User rights or greater

Downloading the Latest Components

After the installation, manually download the latest components (Pattern files\Cleanup templates, Engine updates) from the Trend Micro ActiveUpdate server to help maintain the highest security protection. If a proxy server exists between a Trend Micro server and the Internet, configure the proxy server settings (in the web console, select **Administration** > **Settings** > **Proxy Settings**).

Configuring Event Notifications

After the installation, configure the events that will trigger notifications to monitor significant virus/malware attacks and related security activities. Besides specifying notification recipients, choose notification channels and test them to make sure they work as expected (in the web console, go to **Detections** > **Notifications** > **Event Notifications**).

Chapter 5

Upgrades and Migration

This chapter discusses how to upgrade or migrate to Apex Central from a previous version of Apex Central or Control Manager.

Topics include:

- *Upgrading to Apex Central on page 5-2*
- *Upgrade and Migration Scenarios on page 5-5*
- *Planning Apex Central Agent Migration on page 5-8*
- *Migrating the Apex Central Database on page 5-9*

Upgrading to Apex Central

Migrating a Control Manager installation to Apex Central preserves all your previous settings, logs, reports, Product Directory structure, and integrated Active Directory structure.

Important

- Apex Central only supports upgrading or migrating from Control Manager 6.0 Service Pack 3 Patch 3, Control Manager 7.0, or Control Manager 7.0 Patch 1.
- Before migrating to Apex Central, ensure that your server has sufficient system resources.

  For more information, see *Pre-migration Checklist on page 5-3* or download the *Apex Central System Requirements* PDF document at http://docs.trendmicro.com/en-us/enterprise/apex-central.aspx.

WARNING!

Always back up the existing server before performing the upgrade.

For more information, see *Server Files to Back Up Before Migration on page 5-3*.

Supported Versions for Upgrade

Apex Central supports upgrading from the following versions:

- Control Manager 6.0 Service Pack 3 Patch 3
- Control Manager 7.0
- Control Manager 7.0 Patch 1

WARNING!

Always back up the existing server before performing the upgrade.

Server Files to Back Up Before Migration

Before performing upgrading or migrating a previous Control Manager installation to Apex Central, create a backup of the following server files:

INFORMATION	LOCATION
Database	Use SQL Server Management Studio to back up the database. • For migration from a previous version of Control Manager, the database name is `db_ControlManager`. • For Apex Central, the database name is `db_ApexCentral`.
Authentication information	`\Program Files (x86)\Trend Micro\CmKeyBackup\*.*` (Ensures that managed products reporting to the Apex Central server will report to the same server if Apex Central is restored)
ActiveUpdate files	`\Program Files (x86)\Trend Micro\Control Manager\webui\download\Activeupdate`

Control Manager registry	`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\TVCS`
	`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\CommonCGI`
	`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\TMCM`
	`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer`
	`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TMCM`
	`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrendMicro_NTP`
	`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSSQL$SQLEXPRESS`

Pre-migration Checklist

Before upgrading or migrating Control Manager to Apex Central, ensure that your system satisfies the following minimum requirements.

Important

- Apex Central only supports upgrading or migrating from Control Manager 6.0 Service Pack 3 Patch 3, Control Manager 7.0, or Control Manager 7.0 Patch 1.
- For complete system requirements and supported Windows Server and Microsoft SQL Server versions, download the *Apex Central System Requirements* document from http://docs.trendmicro.com/en-us/enterprise/apex-central.aspx.

Item	Minimum Requirement
Operating System	Windows Server 2012 **Important** If you are running Control Manager on an operating system that is older than Windows Server 2012, you will need to upgrade or migrate to Windows Server 2012 or another supported version.
Available Disk Space	10 GB minimum 80 GB recommended (SAS) **Note** If you are running Control Manager on a server with less than 10 GB of available disk space, you will need to migrate to server with at least 10 GB (80 GB recommended) of available disk space.
SQL Server	Microsoft SQL Server 2008 **Important** Ensure that the SQL Server is running prior to migration.

Item	Minimum Requirement
Trend Micro Services	Ensure that the following services are running prior to migration: • Trend Micro Control Manager • Trend Micro Management Infrastructure

Upgrade and Migration Scenarios

Apex Central supports the following migration scenarios.

- *Scenario 1: Upgrading a Control Manager Server to Apex Central on page 5-5*
- *Scenario 2: Migrating to a Fresh Apex Central Installation Using the Agent Migration Tool on page 5-7*

Upgrade Flow

To upgrade a previous version of Control Manager to Apex Central, run the installation program (`Trend Micro Apex Central.exe`) as described in step 1 of *Installing All Required Components on page 3-10*.

Important

Apex Central only supports upgrading or migrating from Control Manager 6.0 Service Pack 3 Patch 3, Control Manager 7.0, or Control Manager 7.0 Patch 1.

Scenario 1: Upgrading a Control Manager Server to Apex Central

When upgrading a previous version of Control Manager directly to Apex Central, administrators can choose to back up the previous Control Manager installation or back up the entire operating system of the server on which Control Manager installs. Backing up the operating system is more labor intensive but provides better security to prevent data loss.

Important

Apex Central only supports upgrading or migrating from Control Manager 6.0 Service Pack 3 Patch 3, Control Manager 7.0, or Control Manager 7.0 Patch 1.

Upgrading by Backing Up the Previous Control Manager Server and Database

Important

Apex Central only supports upgrading or migrating from Control Manager 6.0 Service Pack 3 Patch 3, Control Manager 7.0, or Control Manager 7.0 Patch 1.

Procedure

1. Back up the previous Control Manager database.
2. Back up all the files under `\Trend Micro\CmKeyBackup\*.*`.
3. Back up all folders of the previous Control Manager server.
4. Back up the registries of the previous Control Manager server.
5. Install Apex Central over Control Manager.

Upgrading by Backing Up the Entire Operating System of the Server and the Apex Central Database

Important

Apex Central only supports upgrading or migrating from Control Manager 6.0 Service Pack 3 Patch 3, Control Manager 7.0, or Control Manager 7.0 Patch 1.

Procedure

1. Back up the operating system of existing Control Manager server.

2. Back up the existing Control Manager database.

3. Install Apex Central over Control Manager.

Scenario 2: Migrating to a Fresh Apex Central Installation Using the Agent Migration Tool

This scenario involves installing Apex Central on a separate server from the existing Apex Central / Control Manager server. This method allows you to slowly decommission the previous server. See *Planning Apex Central Agent Migration on page 5-8* for more information about migrating agents.

Important

Apex Central only supports upgrading or migrating from Control Manager 6.0 Service Pack 3 Patch 3, Control Manager 7.0, or Control Manager 7.0 Patch 1.

Migrating a Control Manager Server to a Fresh Installation of Apex Central

Important

Apex Central only supports upgrading or migrating from Control Manager 6.0 Service Pack 3 Patch 3, Control Manager 7.0, or Control Manager 7.0 Patch 1.

Procedure

1. Back up the existing Control Manager database.

2. Perform a fresh installation of Apex Central on a different computer.

3. Use the Agent Migration Tool to migrate entities from the Control Manager server to the Apex Central server.

Planning Apex Central Agent Migration

There are two ways to migrate agents to a Apex Central server:

- Rapid upgrade
- Phased upgrade

Rapid Upgrade

Rapid upgrade works using the approach presented in the table below.

Table 5-1. Rapid Upgrade

Original Server/ Agent	Action
Control Manager 6.0 Service Pack 3 Patch 3 with MCP agents	Register MCP agents to the Apex Central server and then re-organize the Product Directory structure
Control Manager 7.0 with MCP agents	
Control Manager 6.0 Service Pack 3 Patch 3 with mixed agents Control Manager 7.0 with mixed agents	Register MCP agents to the Apex Central server and then re-organize Product Directory structure

Trend Micro recommends rapid upgrade for migrating agents in a laboratory setting or in relatively small networks, preferably during test deployments (see *Testing Apex Central at One Location on page 2-9*). However, since you cannot stop the migration once it starts, this method works best for smaller deployments. The degree of difficulty increases with the size of the network.

Phased Upgrade

Trend Micro recommends a phased upgrade for large, single-server Control Manager 6.0 Service Pack 3 Patch 3 or 7.0 networks. This is essential for multiple-server networks. This method offers a more structured approach to migrating your system, and follows these guidelines:

- Start migration on systems with the least impact on the existing network, and then proceed to the systems with progressively greater impact
- Upgrade the old network in well-planned stages, rather than all at once

  This will simplify any troubleshooting that may be required.

Phased upgrade involves the following steps:

1. Install Apex Central on a server that does not have any previous Control Manager version installed (preferably without any managed products).
2. Run the `AgentMigrateTool.exe` tool on the Apex Central server.

Use the Apex Central agent installation together with the Agent Migration tool to plan the upgrade of agents on existing Apex Central networks. The Agent Migration tool can generate a list of servers with Apex Central agents. Doing so eliminates the need to manually select the agent servers.

Migrating the Apex Central Database

To migrate a preexisting database for Control Manager 6.0 SP3 Patch 3 or 7.0, install Apex Central on the Control Manager server.

The Apex Central setup program automatically upgrades the database version.

Migrating a Apex Central SQL Database to Another SQL Server

To move a Apex Central database from an SQL Server to another SQL Server, use the DBConfig tool to perform the migration.

Using the Database Configuration Tool (DBConfig.exe)

The `DBConfig.exe` tool allows users to change the user account, password, and the database name for the Apex Central database.

The tool offers the following options:

- **DBName:** Database name
- **DBAccount:** Database account
- **DBPassword:** Database password
- **Mode:** Database authentication mode (SQL Server Authentication or Windows Authentication)

> **Note**
>
> The default database authentication mode is SQL Server Authentication mode. However, Windows Authentication mode is necessary when configuring for Windows authentication.

Procedure

1. Open a command prompt on the Apex Central server.
2. Use the following command to locate the directory which contains the `DBConfig.exe` file:

   ```
   cd <Apex Central installation directory>\DBConfig
   ```

3. Type `dbconfig` and press `ENTER`.

   The DBConfig tool interface appears.

4. Specify which settings you want to modify:

   - Example 1: `DBConfig -DBName="db_your_database>" -DBAccount="sqlAct" -DBPassword="sqlPwd" -Mode="SQL"`
   - Example 2: `DBConfig -DBName="db_your_database>" -DBAccount="winAct" -DBPassword="winPwd" -Mode="WA"`

- **Example 3:** `DBConfig -DBName="db_your_database>" -DBPassword="sqlPwd"`

Chapter 6

Post-Migration Tasks

Perform the following tasks to verify a successful upgrade or migration, import settings from the Apex One server, or enable and configure additional features.

- *Verifying a Successful Upgrade or Migration on page 6-2*
- *Migrating Apex One Server Settings to Apex Central on page 6-3*
- *Enabling Application Control on page 6-4*
- *Enabling Vulnerability Protection on page 6-6*
- *Enabling Endpoint Sensor on page 6-7*
- *Configuring Apex One Server Settings for Endpoint Sensor on page 6-9*

Verifying a Successful Upgrade or Migration

Perform the following procedure to verify that the previous version of Control Manager successfully upgraded to Apex Central.

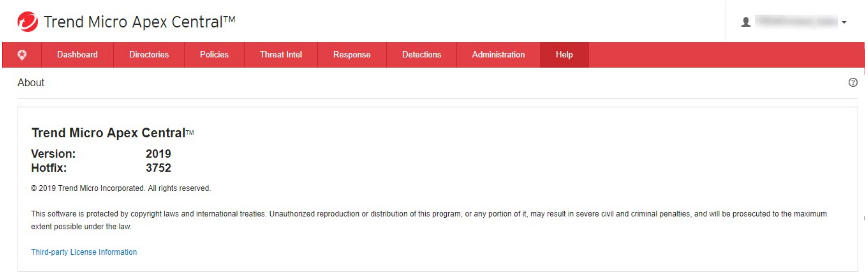
Procedure

1. Log on to the Apex Central web console.

   The Apex Central web console successfully logs on and the **Dashboard** appears.

2. Go to **Help** > **About**

   The **About** screen appears and displays the Apex Central product name and **Version**.

   Trend Micro Apex Central™

   Version: 2019
   Hotfix: 3752

   © 2019 Trend Micro Incorporated. All rights reserved.

   This software is protected by copyright laws and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

   Third-party License Information

3. On the Apex Central server, verify that the following services are running:

   - Trend Micro Apex Central
   - Trend Micro Management Infrastructure

Migrating Apex One Server Settings to Apex Central

Perform the following procedure to migrate existing settings from an existing Apex One server to Apex Central.

Procedure

1. Export settings from the Apex One server.

    a. From the Apex One server, log on to the Apex One web console.

    b. Go to **Administration** > **Settings** > **Server Migration**.

    c. Download the **Apex One Settings Export Tool** to the Apex One server.

    d. Run the `ApexOneSettingsExportTool.exe` program to export settings from the Apex One server.

    e. Copy the export package (`*.zip` file) to a location that is accessible by the Apex Central server.

2. Import the Apex One server settings.

    a. From the Apex Central server, log on to the Apex Central web console.

    b. Go to **Policies** > **Policy Management**.

    c. Select **Apex One Security Agent** as the **Product**.

    d. Click **Import Settings**.

    e. Select and upload the `*.zip` file exported from the Apex One server.

    The screen refreshes and displays the imported policy at the top of the list.

    f. (Optional) Click the policy to edit the settings or perform the following tasks:

- *Enabling Application Control on page 6-4*
- *Enabling Vulnerability Protection on page 6-6*
- *Enabling Endpoint Sensor on page 6-7*

Enabling Application Control

Important

The Application Control feature requires special licensing. Ensure that you have the correct Activation Code before deploying Application Control policies to endpoints. For more information on how to obtain the Activation Code, contact your sales representative.

Procedure

1. Deploy the Activation Code to the managed product servers:

    a. Go to **Administration** > **License Management** > **Managed Products**.

    The **License Management** screen appears.

    b. Click **Add and Deploy**.

    The **Add and Deploy a New License > Step 1: Input Activation Code** screen appears.

    c. Type the Activation Code for the product you want to activate in the **New activation code** field.

    d. Click **Next**.

    The **Add and Deploy a New License > Step 2: Select Targets** screen appears.

    e. Select the target Apex One server(s) to deploy the Activation Code.

    f. Click **Deploy**.

The **License Management** screen appears and the **Activated Products** column displays the number of managed product servers that have successfully deployed the Activation Code.

2. Go to **Policies** > **Policy Management**.

   The **Policy Management** screen appears.

3. Select **Apex One Security Agent** as the **Product**.

4. Specify or edit the **Policy Name**.

5. Specify targets.

6. Create or edit a policy.

   a. To create a policy, click **Create**.

   b. To edit a policy, click a policy name in the **Policy** column.

7. Expand **Application Control Settings**.

8. Select **Enable Application Control**.

9. Click **Deploy** or **Save**.

   The **Policy Management** screen appears and displays the policy deployment status.

   Note

   Deployment times vary depending on the size of your network environment. It may take some time to finish deploying the policy to all specified targets.

Enabling Vulnerability Protection

Important

The Vulnerability Protection feature requires special licensing. Ensure that you have the correct Activation Code before deploying Vulnerability Protection policies to endpoints. For more information on how to obtain the Activation Code, contact your sales representative.

Procedure

1. Deploy the Activation Code to the managed product servers:

   a. Go to **Administration** > **License Management** > **Managed Products**.

      The **License Management** screen appears.

   b. Click **Add and Deploy**.

      The **Add and Deploy a New License > Step 1: Input Activation Code** screen appears.

   c. Type the Activation Code for the product you want to activate in the **New activation code** field.

   d. Click **Next**.

      The **Add and Deploy a New License > Step 2: Select Targets** screen appears.

   e. Select the target Apex One server(s) to deploy the Activation Code.

   f. Click **Deploy**.

      The **License Management** screen appears and the **Activated Products** column displays the number of managed product servers that have successfully deployed the Activation Code.

2. Go to **Policies** > **Policy Management**.

   The **Policy Management** screen appears.

3. Select **Apex One Security Agent** as the **Product**.
4. Specify or edit the **Policy Name**.
5. Specify targets.
6. Create or edit a policy.

    a. To create a policy, click **Create**.

    b. To edit a policy, click a policy name in the **Policy** column.

7. Expand **Vulnerability Protection Settings**.
8. Select **Enable Vulnerability Protection**.
9. Click **Deploy** or **Save**.

    The **Policy Management** screen appears and displays the policy deployment status.

    Note

    Deployment times vary depending on the size of your network environment. It may take some time to finish deploying the policy to all specified targets.

Enabling Endpoint Sensor

Important

- The Endpoint Sensor feature requires special licensing and additional system requirements. Ensure that you have the correct license before deploying Endpoint Sensor policies to endpoints. For more information on how to obtain licenses, contact your support provider.
- Connected Apex One servers require additional hardware and software requirements for the Endpoint Sensor feature to work. For more information, refer to the Apex One Installation and Upgrade Guide.

Procedure

1. Deploy the Activation Code to the managed product servers:

    a. Go to **Administration** > **License Management** > **Managed Products**.

    The **License Management** screen appears.

    b. Click **Add and Deploy**.

    The **Add and Deploy a New License > Step 1: Input Activation Code** screen appears.

    c. Type the Activation Code for the product you want to activate in the **New activation code** field.

    d. Click **Next**.

    The **Add and Deploy a New License > Step 2: Select Targets** screen appears.

    e. Select the target Apex One server(s) or Apex One (Mac) servers to deploy the Activation Code.

    f. Click **Deploy**.

    The **License Management** screen appears and the **Activated Products** column displays the number of managed product servers that have successfully deployed the Activation Code.

2. Go to **Policies** > **Policy Management**.

    The **Policy Management** screen appears.

3. Select **Apex One Security Agent** as the **Product**.

4. Specify or edit the **Policy Name**.

5. Specify targets.

6. Create or edit a policy.

    a. To create a policy, click **Create**.

b. To edit a policy, click a policy name in the **Policy** column.

7. Expand **Endpoint Sensor Settings**.

8. Select **Enable Endpoint Sensor**.

9. Click **Deploy** or **Save**.

   The **Policy Management** screen appears and displays the policy deployment status.

   Note

   Deployment times vary depending on the size of your network environment. It may take some time to finish deploying the policy to all specified targets.

Configuring Apex One Server Settings for Endpoint Sensor

Important

- The Endpoint Sensor feature requires special licensing and additional system requirements. Ensure that you have the correct license before deploying Endpoint Sensor policies to endpoints. For more information on how to obtain licenses, contact your support provider.

- Connected Apex One servers require additional hardware and software requirements for the Endpoint Sensor feature to work. For more information, refer to the Apex One Installation and Upgrade Guide.

- The following procedure assumes you have already enabled Endpoint Sensor by creating or editing an Apex One Security Agent policy.

  For more information, see *Enabling Endpoint Sensor on page 6-7*.

Procedure

1. Go to **Policies** > **Policy Management**.

   The **Policy Management** screen appears.

2. Select **Apex One Server** as the **Product**.

3. Specify or edit the **Policy Name**.

4. Specify targets.

5. Create or edit a policy.

   a. To create a policy, click **Create**.

   b. To edit a policy, click a policy name in the **Policy** column.

6. Expand **Endpoint Sensor** to configure the following settings:

Option	Description
Maximum metadata storage	Specify the maximum size allowed for metadata storage. Specify a size between 1024 to 4096 GB. The default storage size is 1024 GB. Once the metadata storage reaches this size, the server purges old records to accommodate new ones.
Maximum memory allocation	Specify the maximum amount of memory allocated to the metadata cache. Specify a size between 4 GB and 64 GB. The new size specified must be higher than the current size. The default allocation size is 4 GB. **Note** Memory size affects the performance of data uploads and investigation speed. To improve performance, increase the memory size of the affected server.

7. Click **Deploy** or **Save**.

   The **Policy Management** screen appears and displays the policy deployment status.

Note

Deployment times vary depending on the size of your network environment. It may take some time to finish deploying the policy to all specified targets.

Chapter 7

Uninstallation

This chapter contains information about how to uninstall Apex Central and remove related files.

Topics include:

- *Removing Apex Central on page 7-2*
- *Manually Removing Apex Central on page 7-3*

Removing Apex Central

Uninstall Apex Central from the server by using one of the following methods:

Procedure

- From the **Start** menu, click **Start** > **Trend Micro Apex Central** > **Uninstalling Trend Micro Apex Central**.
- Using **Add/Remove Programs**:

  a. Go to **Start** > **Control Panel** > **Add/Remove Programs.**

  b. Select **Trend Micro Apex Central** and click **Uninstall**.

     A confirmation dialog appears.

  c. Click **Yes** to uninstall Apex Central.

  d. Choose whether to uninstall the Apex Central database:

     Note

     Keeping the database allows you to reinstall Apex Central on the server and retain all system information, such as agent registration and user account data.

     - To uninstall the database, select the **Remove Apex Central database** check box.
     - To keep the database, do not select the **Remove Apex Central database** check box.

  e. Click **Next.**

     - The uninstallation program removes Apex Central from the server.
     - If you selected **Remove the Apex Central database**, the uninstallation program also removes the database.

- If you reinstall the Apex Central server without deleting the original database and removing the managed products that originally reported to the previous server, then the managed products will re-register to the Apex Central server when:
  - Managed product servers restart MCP agent services
  - MCP agents verify their connection after an 8-hour period

Manually Removing Apex Central

This section describes how to remove Apex Central manually. Use the procedures below only if the Windows Add/Remove function or the Apex Central uninstall program is unsuccessful.

Note

Windows-specific instructions may vary between operating system versions. The following procedures are written for Windows Server 2012.

Removing Apex Central actually involves removing distinct components. These components may be removed in any order; they may even be removed together. However, for purposes of clarity, the uninstallation for each module is discussed individually, in separate sections. The components are:

- Apex Central application
- Apex Central Database (optional)

Note

After removing all components, you must restart your server. You only have to do this once — after completing the removal.

Removing the Apex Central Application

Manual removal of the Apex Central application involves the following steps:

1. *Stopping Apex Central Services on page 7-4*
2. *Removing Apex Central IIS Settings on page 7-5*
3. *Deleting Apex Central Files/Directories and Registry Keys on page 7-6*
4. *Removing the Database Components on page 7-7*
5. *Removing the Apex Central Service on page 7-8*

Stopping Apex Central Services

Use the **Windows Services** screen to stop all of the following Apex Central services:

- Trend Micro Apex Central

Note

These services run in the background on the Windows operating system, not the Trend Micro services that require Activation Codes (for example, Outbreak Prevention Services).

Stopping Apex Central Services from the Windows Services Screen

Procedure

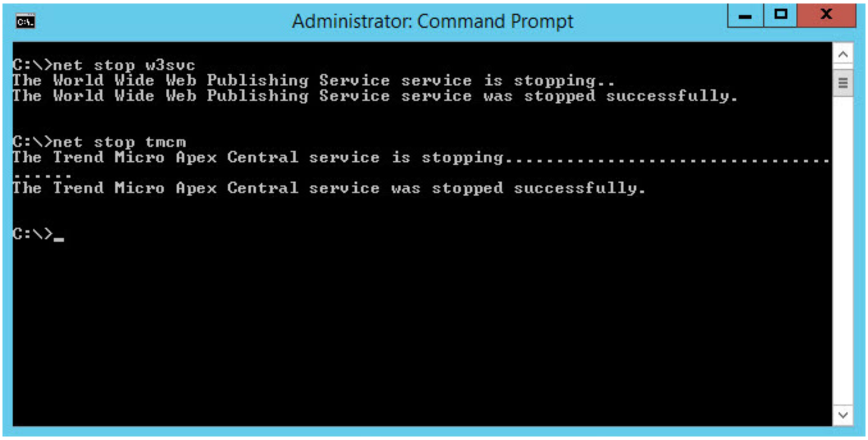
1. Click **Start** > **Programs** > **Administrative Tools** > **Services** to open the **Services** screen.
2. Right-click **Trend Micro Apex Central** and then click **Stop**.

Stopping IIS and Apex Central Services from the Command Prompt

Procedure

- Run the following commands at the command prompt:

```
net stop w3svc
net stop tmcm
```



```
C:\>net stop w3svc
The World Wide Web Publishing Service service is stopping..
The World Wide Web Publishing Service service was stopped successfully.

C:\>net stop tmcm
The Trend Micro Apex Central service is stopping................................
......
The Trend Micro Apex Central service was stopped successfully.

C:\>_
```

FIGURE 7-1. View of the command line with the necessary services stopped

Removing Apex Central IIS Settings

Remove the Internet Information Services settings after stopping the Apex Central services.

Procedure

1. From the Apex Central server, click **Start** > **Run**.

   The **Run** dialog box appears.

2. Type the following in the **Open** field:

   ```
   %SystemRoot%\System32\Inetsrv\iis.msc
   ```

3. On the left-hand menu, double-click the server name to expand the console tree.

4. Double-click **Default Web Site**.

5. Delete the following virtual directories:

    - `ControlManager`
    - `TVCSDownload`
    - `TVCS`
    - `WebApp`

6. Select the **ISAPI Filters** tab.

7. Delete the following ISAPI filters:

    - TmcmRedirect
    - ReverseProxy

Deleting Apex Central Files/Directories and Registry Keys

Procedure

1. Delete the following directories:

    - `.Trend Micro\Control Manager`
    - `.PHP`
    - `C:\Documents and Settings\All Users\Start Menu\Programs\PHP 7`
    - `C:\Documents and Settings\All Users\Start Menu\Programs\Trend Micro Apex Central`

2. Delete the following Apex Central registry keys:

    - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\MCPAgent`
    - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OPPTrustPort`
    - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TMI`

- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TVCS`
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TMCM`

Removing the Database Components

This section describes how to remove the following database components from the Apex Central server:

- *Removing Apex Central ODBC Settings on page 7-7*
- *Removing the SQL Server 2017 Express Database on page 7-7*

Removing Apex Central ODBC Settings

Procedure

1. On the Apex Central server, click **Start** > **Run**.

   The **Run** dialog box appears.

2. Type the following in the **Open** field:

   `odbcad32.exe`

3. On the **ODBC Data Source Administrator** screen, click the **System DSN** tab.

4. Under **Name**, select **ControlManager_Database**.

5. Click **Remove**, and then click **Yes** to confirm.

Removing the SQL Server 2017 Express Database

Procedure

1. On the Apex Central server, click **Start** > **Control Panel** > **Add/Remove Programs**.

2. Scroll down to **SQL Server 2017** and then click **Remove** to remove the related files automatically.

> **Tip**
>
> For more information on removing SQL Server 2017 Express, refer to the Microsoft documentation.

Removing the Apex Central Service

Procedure

1. Run the Microsoft service tool `Sc.exe`.

2. Type the following command:

```
sc delete "TMCM"
```

Chapter 8

Apex Central System Checklists

Use the checklists in this section to record relevant system information as a reference.

Topics include:

- *Server Address Checklist on page 8-2*
- *Port Checklist on page 8-3*
- *Apex Central Conventions on page 8-4*
- *Core Processes and Configuration Files on page 8-4*
- *Communication and Listening Ports on page 8-6*

Server Address Checklist

You must provide the following server address information during the installation process, as well as during the configuration of the Apex Central server to work with your network. Record the information here for easy reference.

TABLE 8-1. Server Address Checklist

INFORMATION REQUIRED	EXAMPLE	YOUR VALUE
Apex Central server information		
IP address	10.1.104.255	
Fully qualified domain name (FQDN)	server.company.com	
NetBIOS (host) name	yourserver	
Web server information		
IP address	10.1.104.225	
Fully qualified domain name (FQDN)	server.company.com	
NetBIOS (host) name	yourserver	
SQL-based Apex Central database information		
IP address	10.1.104.225	
Fully qualified domain name (FQDN)	server.company.com	
NetBIOS (host) name	sqlserver	
Proxy server for component download		
IP address	10.1.174.225	
Fully qualified domain name (FQDN)	proxy.company.com	

Information Required	Example	Your Value
NetBIOS (host) name	proxyserver	
SMTP server information (Optional; for email message notifications)		
IP address	10.1.123.225	
Fully qualified domain name (FQDN)	mail.company.com	
NetBIOS (host) name	mailserver	
SNMP Trap information (Optional; for SNMP Trap notifications)		
Community name	trendmicro	
IP address	10.1.194.225	
Syslog server information (Optional; for syslog notifications)		
IP address	10.1.194.225	
Server port	514	

Port Checklist

Apex Central uses the following ports for the indicated purposes.

Port	Sample	Your Value
SMTP	25	
Proxy	8088	
Web Console and Update/ Deploy components	80	

Apex Central Conventions

Refer to the following conventions applicable for the Apex Central installation or web console configuration.

- User names
  - Max. length: 32 characters
  - Allowed: `A-Z`, `a-z`, `0-9`, `-`, `_`, `.`, `$`
- Folder names
  - Max. length: 32 characters
  - Not allowed: `/`, `>`, `&`, `"`, `%`, `^`, `=`

Note

For the Apex Central server host name, the setup program supports servers with underscores ("_") as part of the server name.

Core Processes and Configuration Files

Apex Central saves system configuration settings and temporary files in XML format.

The following tables describe the configuration files and processes used by Apex Central.

Table 8-2. Apex Central Configuration Files

Configuration File	Description
`AuthInfo.ini`	Configuration file that contains information about private key file names, public key file names, certificate file names, and the encrypted passphrase of the private key as well as the host ID and port.
`aucfg.ini`	ActiveUpdate configuration file

Configuration File	Description
`TVCS_Cert.pem`	Certificate used by SSL authentication
`TVCS_Pri.pem`	Private Key used by SSL
`TVCS_Pub.pem`	Public Key used by SSL
`ProcessManager.xml`	Used by `ProcessManager.exe`
`CmdProcessorEventHandler.xml`	Used by `CmdProcessor.exe`
`DMRegisterinfo.xml`	Used by `CasProcessor.exe`
`DataSource.xml`	Stores the connection parameters for Apex Central processes
`SystemConfiguration.xml`	Apex Central system configuration file
`agent.ini`	MCP agent file

Table 8-3. Apex Central Core Processes

Processes	Description
`ProcessManager.exe`	Launches and stops other Apex Central core processes
`CmdProcessor.exe`	Sends XML instructions, formed by other processes, to managed products, processes product registration, sends alerts, performs scheduled tasks, and applies Outbreak Prevention Policies
`LogReceiver.exe`	Receives managed product logs and messages. Starting with Control Manager 3.0 Service Pack 4, `LogReceiver.exe` only handles logs coming from Trend Micro Damage Control Services and Trend Micro Vulnerability Assessment
`LogProcessor.exe`	Receives logs from managed products, and receives entity information from managed products
`LogRetriever.exe`	Retrieves and saves logs in the Apex Central database
`ReportServer.exe`	Generates Apex Central reports

PROCESSES	DESCRIPTION
`MsgReceiver.exe`	Receives messages from the Apex Central server and managed products
`CasProcessor.exe`	Allows a Apex Central server to manage other Apex Central servers
`inetinfo.exe`	Microsoft Internet Information Service process
`cm.exe`	Manages `dmserver.exe` and `mrf.exe`
`dmserver.exe`	Provides the Apex Central web console log on page and manages the Product Directory (Apex Central-side)
`sCloudProcessor.NET.exe`	Requests the Apex Central web console or other processes to provide a job ID for the issuer to query statuses, query results, and cancel requests; used by the User/Endpoint Directory

Communication and Listening Ports

These are the default Apex Central communication and listening ports.

SERVICE	SERVICE PORT
`ProcessManager.exe`	20501
`CmdProcessor.exe`	20101
`comdProcessor.NET.exe`	21003
`LogReceiver.exe`	20201
`LogProcessor.exe`	21001
`LogRetriever.exe`	20301
`ReportServer.exe`	20601
`MsgReceiver.exe`	20001
`CasProcessor.exe`	20801

Service	Service Port
sCloudProcessor.NET.exe	21002

Index

A

activating
- Apex Central, 4-4

Activation Code, 4-4

Active Directory
- connection settings, 4-5
- manual synchronization, 4-5
- synchronization frequency, 4-5

Apex Central, 1-1, 1-2, 1-5
- about, 1-1, 1-2
- activating, 4-4
- command prompt, stopping service from, 7-4
- installation steps, 3-9
- installing, 3-1, 3-8, 3-9
- license information, 4-4
- mail server, 1-5
- manually removing, 7-3
- MCP, 1-5
- removing manually, 7-3
- report server, 1-5
- SQL database, 1-5
- system requirements, 3-2
- web-based management console, 1-6
- web server, 1-5
- web service integration, 1-5
- widget framework, 1-6

B

backing up Apex Central, 5-3

C

checklist
- ports, 8-3
- server address, 8-2

command polling
- MCP, 2-17

command prompt
- Apex Central, stopping service from, 7-4

configuring
- user accounts, 4-8
- web server, 2-21

Control Manager
- migrating database, 5-9
- security levels, 3-17
- testing pilot deployment, 2-9

converting
- full version, 4-5

D

database
- recommendations, 2-20

data storage
- plan, 2-19

DBConfig tool, 5-10

deployment
- architecture and strategy, 2-2
- multiple-site, 2-4
- single-site, 2-3

documentation, vi

F

full version
- converting, 4-5

H

heartbeat, 2-14
- MCP, 2-17

I

- installation
  - flow, 2-9
  - verify success, 4-2
- installation steps
  - Apex Central, 3-9
- installing
  - Apex Central, 3-1, 3-9
  - steps, 3-9

L

- license information, 4-4
- logs
  - traffic, 2-15

M

- manually
  - removing Apex Central, 7-3
- manually uninstalling, 7-3
- MCP, 1-5
  - command polling, 2-17
  - heartbeat, 2-17
  - policies, 2-17
- migrating, 5-8
  - Control Manager SQL 2000, 5-9
  - database, 5-9
  - phased upgrade, 5-8
  - rapid upgrade, 5-8
  - strategy, 5-8
- multiple-site deployment
  - understanding, 2-4

N

- network traffic
  - sources, 2-15
- network traffic plan, 2-13

O

- ODBC
  - settings, Control Manager, 7-7

P

- phased upgrade, 5-8
- pilot deployment
  - testing, 2-9
- policies
  - MCP, 2-17
- port
  - checklist, 8-3
- product registration
  - traffic, 2-17

R

- rapid upgrade, 5-8
- recommendations
  - database, 2-20
- Registration Key, 4-5
- remove
  - manual
    - Microsoft Data Engine, 7-7
- removing
  - Apex Central manually, 7-3
  - manual
    - Apex Central, 7-3

S

- server
  - address checklist, 8-2
- server address checklist, 8-2
- server distribution plan, 2-11
- single-site deployment
  - understanding, 2-3
- system requirements, 3-2

T

terminology, viii

tools

- DBConfig tool, 5-10

traffic, network, 2-13

U

understanding

- multiple-site deployment, 2-4
- single-site deployment, 2-3

updates

- deploying, 2-18

upgrading, 5-2

- backing up Apex Central information, 5-3

user accounts

- configuring, 4-8

V

verify successful installation, 4-2

W

web server

- configuration, 2-21
- plan, 2-21

web server settings, 3-15

Windows Server 2012, 3-3

Windows Server 2012 R2, 3-4

Windows Server 2016, 3-5

Windows Server 2019, 3-6

Windows Server 2022, 3-7

TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: APEM39503/220311