802.1X Authenticated Wireless Access Overview

Updated: September 18, 2013

Applies To: Windows Server 2012

This document provides introductory information about Institute of Electrical and Electronics Engineers (IEEE) 802.1X authenticated access for IEEE 802.11 wireless access. Links to resources with information about technologies that are closely related to 802.1X authenticated wireless access, or otherwise relevant to wireless access are also provided.

Note

In addition to this topic, the following 802.1X Authenticated Wireless Access documentation for Windows Server 2012 is also available.

- What's New in 802.1X Authenticated Wireless Access
- Improvements to Certificate-based Authentication
- Wireless LAN Service Overview
- Managing the Wireless Network (IEEE 802.11) Policies
- Core Network Companion Guide: Deploying Password-based 802.1X Authenticated Wireless Access
- New Wireless Connection Processes

Did you mean...

- 802.1X Authenticated Wired Access
- Netsh Commands for Wireless Local Area Network (WLAN) in the Windows Server 2008 R2 and Windows Server 2008 technical library on TechNet.
- 802.1X Authenticated Wireless Access in the Windows Server 2008 R2 and Windows Server 2008 technical library on TechNet.

Feature description

IEEE 802.1X authentication provides an additional security barrier for your intranet that you can use to prevent guest, rogue, or unmanaged computers that cannot perform a successful authentication from connecting to your intranet.

For the same reason that administrators deploy IEEE 802.1X authentication for IEEE 802.3 wired networks—enhanced security—network administrators want to implement the IEEE 802.1X standard to help protect their wireless network connections. Just as an authenticated wired client must submit a set of credentials to be validated before being allowed to

send frames over the wired Ethernet intranet, an IEEE 802.1X wireless client must also perform authentication prior to being able to send traffic over its wireless access point (AP) port, and over the network.

Important terminology and technology overviews

Following are overviews that will help you to understand the various technologies that are required to deploy 802.1X authenticated wireless access.

Note
In this document, 802.1X authenticated wireless access is referred to as WiFi access.

IEEE 802.1X

The IEEE 802.1X standard defines the port-based network access control that is used to provide authenticated WiFi access to corporate networks. This port-based network access control uses the physical characteristics of the 802.1X capable wireless APs infrastructure to authenticate devices attached to a LAN port. Access to the port can be denied if the authentication process fails. Although this standard was first designed for wired Ethernet networks, it has also been adapted for use on 802.11 wireless LANs.

IEEE 802.1X-capable wired Ethernet switches

To deploy 802.1X wireless access you must install and configure one or more 802.1X-capable wireless APs on your network. The wireless APs must be compatible with the Remote Authentication Dial-In User Service (RADIUS) protocol.

When 802.1X and RADIUS-compliant wireless APs are deployed in a RADIUS infrastructure, with a RADIUS server such as an NPS server, they are called *RADIUS clients*.

IEEE 802.11 wireless

IEEE 802.11 is a collection of standards that defines the Layer-1 (physical layer) and Layer-2 (data-link layer media access control (MAC)) of WiFi access.

Network Policy Server

Network Policy Server (NPS) lets you centrally configure and manage network policies by using the following three components: RADIUS server, RADIUS proxy, and Network Access Protection (NAP) policy server. NPS is required to deploy 802.1X wireless access.

Server certificates

WiFi access deployment requires server certificates for each NPS server that performs 802.1X authentication.

A *server certificate* is a digital document that is commonly used for authentication and to help secure information on open networks. A certificate securely binds a public key to the entity that holds the corresponding private key. Certificates are digitally signed by the issuing certification authority (CA), and they can be issued for a user, a computer, or a service.

A CA is an entity responsible for establishing and vouching for the authenticity of public keys that belong to subjects (usually users or computers) or other CAs. Activities of a CA can include binding public keys to distinguished names through signed certificates, managing certificate serial numbers, and revoking certificates.

Active Directory Certificate Services (AD CS) is a Windows Server 2012 server role that issues certificates as a network CA. An AD CS certificate infrastructure, also called a *public key infrastructure (PKI)*, provides customizable services for issuing and managing certificates for the enterprise.

EAP

Extensible Authentication Protocol (EAP) extends Point-to-Point Protocol (PPP) by enabling additional authentication methods that use credential and information exchanges of arbitrary lengths. With EAP authentication, both the network access client and the authenticator (such as an NPS server) must support the same EAP type for successful authentication to occur.

New and changed functionality

In Windows Server 2012, WiFi access includes only minimal changes to the wired access solution provided in Windows Server 2008 R2. That change is summarized as follows:

Feature/functionality	Previous operating system	New operating system
The addition of EAP-Tunneled Transport Layer Security (EAP-TTLS) to the list of network authentication methods that are included by default	Not included	Included by default

See also

Following are additional resources that pertain to 802.1X authenticated wireless access.

Content type	References
Product evaluation	Connecting to Wireless Networks with Windows 7 The Cable Guy - July 2010 |

Planning	Windows Server 2008 802.1X Authenticated Wireless Access Design Guide |
Deployment	Windows Server 2008 802.1X Authenticated Wireless Access Deployment Guide | Windows Server 2012 Core Network Companion Guide: Deploying Password-based 802.1X Authenticated Wireless Access | Windows Server 2008 R2 Core Network Companion Guide: Deploying Password-based 802.1X Authenticated Wireless Access
Operations	Windows Server 2012 Managing the Wireless Network (IEEE 802.11) Policies extension of Group Policy| Extensible Authentication Protocol (EAP) Settings for Network Access | Windows Server 2012 Wireless LAN Service Overview| Windows Server 2008 R2 Netsh Commands for Wireless Local Area Network (WLAN) |
Troubleshooting	Windows Server 2008 R2 Network Diagnostics Framework (NDF) and Network Tracing |
Security	Content not available
Tools and settings	Windows Server 2012 Managing the Wireless Network (IEEE 802.11) Policies extension of Group Policy
Community resources	Content not available
Related technologies	Windows Server 2008 R2 *802.1X Authenticated Wired Access* | Windows Server 2008 R2 Network Policy and Access Services