**Module storyboard**

|  |  |
| --- | --- |
| **Credential name** | Cybersecurity |
| **Module name** | Network Security |
| **Contributors** | * ID(s): Marty Hale-Evans
* Lead ID: Zachary Rash
* SME(s): Dee Dee Collette
* Assessment: Brandi Robinson
* Editor/QA: US Editors
 |
| **Readability – Grade level)** | 11.3 |
| **Readability – Passive sentences** | 8.7% |

Module content

[Lesson 4: Network access control 3](#_Toc133586632)

[About this lesson: Network access control 3](#_Toc133586633)

[What is network access control? 3](#_Toc133586634)

[Identification, authentication, authorization, and accounting 3](#_Toc133586635)

[Authentication and authorization 4](#_Toc133586636)

[Access control schemes 6](#_Toc133586637)

[File system permissions 7](#_Toc133586638)

[Career highlight: Identity and Access Management Specialist 8](#_Toc133586639)

[Summary and looking ahead 8](#_Toc133586640)

# Lesson 4: Network access control

## About this lesson: Network access control

Any system can only be secure if the people using it can be trusted. If a network allows in the wrong users or allows them access to the wrong assets and resources, the risk of attack and damage grows immensely.

In this lesson, you’ll learn how admins can set up systems that help ensure that the right people can get to the resources that they need and keep the system safe.

|  |
| --- |
| **Developer note:** The lesson-level objectives here will not appear in the programmed module; they are here to guide the instructional designer and assessment specialist.Learning objectivesAfter completing this lesson, you should be able to:* Differentiate between network access controls
* Identify authentication methods
 |

## What is network access control?

To maintain a secure system, users and admins must ensure that only trusted users can access the network and its resources. They must build the system so that only the right users enter the network and potential attackers stay out.

**Developer note:** Definition block

**Network access control (NAC)** controls and manages access to a network by authenticating users and devices before allowing them to connect.

**Developer note:** End definition block

Network access control is a vital part of network security. It helps to prevent unauthorized access to network resources and reduces the risk of data breaches and cyberattacks. It also helps to ensure compliance with security policies and regulations.

## Identification, authentication, authorization, and accounting

Admins use **identification**, **authentication**, **authorization**, and **accounting** (IAAA) to control access to resources and to protect sensitive information. Data confidentiality, integrity, and availability all depend on identification, authentication, authorization, and accounting.

Select each tab to learn more.

**Developer note:** Tab interaction

**Graphic Note**: Each tab will contain a variation of the same scene: people waiting in line to get into a club, with a bouncer at the door.

Identification

**Graphic Note**: In this variation, the bouncer looks at the first person in line, perhaps with a dotted sight line.

In identification, the system tries to recognize a user or a device that attempts to access a system or resource. It might do this with usernames, employee IDs, or IP addresses.

Think about someone trying to enter an exclusive club. It helps their chances to get in if the bouncer at the door recognizes who they are.

Authentication

**Graphic Note**: The bouncer checks the person’s ID.

In authentication, the system tries to verify the identity of a user or device to make sure they really are who they claim to be. It might ask for passwords or biometric data.

If someone tries to get into a club, the bouncer will likely ask to see ID, even if they recognize the person’s face.

Authorization

**Graphic Note**: The bouncer checks a clipboard list.

In authorization, the system checks the user’s privileges and grants or denies access to resources based on the authenticated identity of the user or device. When a user is authenticated, they will only receive access to the resources that they are authorized to access.

Even if the bouncer recognizes someone getting and has checked their ID, the bouncer will check their list to see where that person is allowed to go in the club.

Accounting

**Graphic Note**: The scene has security cameras now, emphasize them.

The accounting process tracks and records user activity and resource usage. This supplies a means to track and trace access and usage for specific users and devices, which may help detect security breaches or company policy violations. Some examples include logging user sessions, logging access attempts, and logging resource usage.

The process of getting into a club and the person’s activity in the club may be recorded by security footage in case someone needs to follow up on a later situation.

**Developer note:** End tab interaction

Take a moment to think about the types of network access controls on your accounts. At the end of this lesson, you will use these terms to complete a crossword puzzle. Consider recording their definitions on a notes page to help you with the puzzle.

## Authentication and authorization

Authentication verifies the identity of a user or device, while authorization determines what actions the authenticated user or device can perform on the system or resource. In combination, authentication and authorization validates your identity before granting you access to the systems, resources, and other network assets that you need. Every system requires this combination as fundamental to its security.

Watch the following video to learn more about authentication and authorization.

**Developer note:** Insert video: Authentication and authorization (once we have it)

**Reviewer note:** Link to video script: <https://ibm.box.com/s/f6laksjed19ut4w1gmrfnoqdijbr5gr0>

**Developer note:** Insert link to the transcript’s PDF (once we have it).

Now that you’re familiar with authentication and authorization, you’re ready to explore it in more detail.

### Additional authentication methods

Usernames and passwords traditionally give basic authentication, and many systems still use them, However, most modern systems use additional methods of authentication for a higher level of protection.

Select each card to learn more.

**Developer note:** Flashcard grid

**Card 1**

Front:

Knowledge-based authentication

Back:

Knowledge-based authentication

Knowledge-based authentication (KBA) verifies the identity of a user by asking questions based on information that only the user knows, such as a secret question or a personal identification number.

**Card 2**

Front:

Single sign-on

Back:

Single sign-on

Single sign-on (SSO) enables users to access multiple resources with one set of login credentials. The SSO portal fully authenticates the user and creates a certificate or token that acts as a security key for other resources.

**Card 3**

Front:

Multifactor authentication

Back:

Multifactor authentication

Multifactor authentication (MFA) requires users to provide two or more authentication factors to prove their identities. Some examples might be a security code sent to a phone, a physical cardkey, or a fingerprint scan.

**Card 4**

Front:

Adaptive authentication

Back:

Adaptive authentication

Adaptive authentication, also known as risk-based authentication, changes authentication requirements in real time when needed. A user logging in from a usual device may only need to enter a username and password. If the same user connects from an untrusted device or tries to view sensitive information, the system may require additional authentication factors.

**Developer note:** End flashcard grid

### Knowledge check

**Developer note**: In line on page. Set to must attempt.

1. When a website asks a user to answer security questions such as "What is your mother's maiden name?" or "What city were you born in?" to verify their identity and grant access to their account. This is an example of which type of authentication?

Adaptive authentication

Single sign-on authentication

Multifactor authentication

**Knowledge-based authentication**

Feedback [Correct]: Correct! Knowledge-based authentication is when a user answers security questions such as "What is your mother's maiden name?" or "What city were you born in?" to verify their identity and grant access to their account.

Feedback [Incorrect]: Not quite. The user's knowledge is specific to the type of authentication.

2. When a user logs into their online banking account, they are prompted to enter their login credentials as well as a code sent to their mobile device. This is an example of which type of authentication?

Adaptive authentication

Single sign-on authentication

**Multifactor authentication**

Knowledge-based authentication

Feedback [Correct]: Correct! The combination of something they know (the login credentials) and something they have (the mobile device) creates a multi-factor authentication.

Feedback [Incorrect]: Not quite. The user needs knowledge and another factor to authenticate.

**Developer note**: End Knowledge Check.

## Access control schemes

Managing access control for a handful of users using a few devices isn’t too hard. However, managing access control across hundreds or thousands of users and devices can be incredibly challenging.

**Developer note:** Definition block

**Access control schemes** help provide consistency in access control to network resources.

**Developer note:** End definition block

Access control schemes ensure that only authorized users can access the resources they need. They also prevent unauthorized access, theft, and damage.

There are four primary access control schemes that can be used, depending on the system's security requirements.

***Select each section to learn more.***

**Developer note:** Accordion

Attribute-based access control (ABAC)

**Graphic Note**: Different types of attributes feed into a decision module showing policies, see [this](https://www.archtis.com/wp-content/uploads/2023/01/ABAC.png).

**Attribute-based access control (ABAC) systems** base access control decisions on attributes that define the user, the resource, and the environment where users are requesting access. These attributes can include factors like the user’s job title, location, or time of day. Based on how these attributes match predefined policies, the system grants or denies access.

Role-based access control (RBAC)

**Graphic Note**: A few users with different roles (manager, accountant, and consultant for example), and some resources, showing with connections that different roles can access different resources.

**Role-based access control (RBAC) systems** determine access control decisions based on the roles assigned to users or groups. Admins assign roles to users based on business functions, and the system grants access rights based on those roles instead of individual attributes.

Discretionary access control (DAC)

**Graphic Note**: An owner and users, the owner deciding who can access a resource, see [this](https://assets.website-files.com/5ff66329429d880392f6cba2/60a23b8db2d312810b7c34d8_Discretionary%20Access%20Control%20%28DAC%29.png).

In **discretionary access control (DAC)** systems, every object or resource in the system has an owner who determines which users can access it. The owner can grant or deny access to other users based on their own discretion.

Mandatory access control (MAC)

**Graphic Note**: Users and a hierarchy of control levels they need to access resources, see [this](https://www.researchgate.net/publication/358430862/figure/fig4/AS%3A1121209311866928%401644328539489/view-of-mandatory-access-control-MAC.jpg).

In **mandatory access control (MAC)** systems, users do not have control over their own access rights. Instead, a central authority such as a security administrator regulates what access rights each user has based on predetermined rules and policies. These usually create a tiered, hierarchical access structure.

**Developer note:** End accordion

## File system permissions

While many access control methods evaluate users and their attributes, some are connected to the resources themselves.

**Developer note:** Definition block

**Filesystem controls** determine which accounts, users, groups, or services can perform actions like reading, writing, and running files.

**Developer note:** Definition block

Each operating system has its own set of filesystem permissions and capabilities for control, as well as its own interface for working with them. The interface for the Windows filesystem, for example, looks something like the following picture. Windows filesystem permissions can be applied to files or folders individually or inherited from parent folders. Permissions can be granted or denied to individual users or groups and can be changed or removed at any time.

Let’s explore the various permissions that you can adjust from the Windows filesystem permissions interface.

***Select each marker (+) on the following graphic to learn more.***

Developer note: Labeled graphic. Use the following as a guide. Put a + symbol next to each list item.

**Alt text**: A diagram shows a screenshot of the Windows filesystem permissions interface.



Full control

+ The full control option allows the user to perform any action on a file or folder, including taking ownership, changing permissions, or deleting it.

Modify

+ The modify option allows users to perform any action on files or folders, except for taking or changing ownership.

Read and execute

+ The read and execute option allows a user to view the contents of a file or folder, but not the content of its subfolders.

Read

+ The read option allows a user to only view the contents of a file or folder.

Write

+ The write option allows a user to make changes to a file or folder.

Special permissions

+ The special permissions option enables an admin to create an exception or specific permission based on some user attribute.

**Developer note:** End labeled graphic

## Activity: Differentiate between network access controls

**Developer note:** H5P Crossword Puzzle

Clue:

1. Employees are assigned roles like "sales representative" or "finance manager" to determine their access level to company resources in the computer system.

**Role**

2. A user enters login credentials and a texted code. The system verifies the entry before granting access to their account information and transactions.

**Authentication**

3. The system checks user or device privileges to determine allowed access.

**Authorization**

4. When accessing a sensitive document, the system logs the employee's user ID, and access time for auditing, compliance, and security.

**Accounting**

5. An access control based on clearance level, job function, and area sensitivity, with the security administrator regulating access to different areas.

**Mandatory**

6. After authenticating an employee, the system checks their access level to grant or deny entry to a specific database in the company's network.

**Authorization**

**Mockup**: <https://csr.h5p.com/content/1291943269423459368>

Developer note: End H5P

## Career highlight: Identity and access management specialist

**Developer note:** Use [Career\_Management\_Skills\_Unlabeled.png](https://app.box.com/file/1161671990892?s=2e7j8loxixpudjxb2ytxvrid8cv47y8a). Align to the left.

An identity and access management analyst manages and secures user access to company resources such as computer systems, networks, and applications. Their primary duty is to ensure only authorized users have access to sensitive information. They work closely with IT and security teams to establish controls, monitor activity, and proactively mitigate security threats.

Identity and access management analysts must understand their employer’s requirements, policies, and procedures. Typically, they must perform the following tasks:

* Identify areas of risk
* Develop solutions that balance security and usability
* Design, implement, and maintain access control systems and processes
* Work collaboratively with other stakeholders

## Summary and looking ahead

**Developer note:** Use the appropriate content treatment for this page.

In this lesson, you learned how network control keeps a system safe, and some common access control schemes. You’ve learned about identification, authentication, authorization, and accounting, as well as some authentication practices.

You’ve completed the final lesson of this module. Next, you’ll review the module’s key points and explore additional resources related to network security.